This document provides **interim**[[1]](#footnote-1) guidance to clarify **current** requirements for the disclosure of VA research data to academic affiliates and other non-VA entities for “collaborative” human subject research.[[2]](#footnote-2) This guidance is intended to facilitate implementation of the principles articulated by the *Working Group on Information Technology Security and Privacy in VA and NIH-Sponsored Research* (Association of American Medical Colleges, November 2010) [hereafter, “*Working Group* report”]*.*[[3]](#footnote-3)

Collaborative studies with non-VA entities pose distinct challenges related to records retention, the disclosure of data under the Health Insurance Portability and Accountability Act (HIPAA), data ownership, and data security, each of which requires consideration relative to collaborative research arrangements.

**Record Retention**

1. VA must retain the complete record (i.e., original or copy) of alldata obtained in VA research in accordance with privacy requirements,[[4]](#footnote-4),[[5]](#footnote-5) the Federal Records Act, and applicable federal records retention requirements.[[6]](#footnote-6),[[7]](#footnote-7) This complete record must be readily accessible for inspection by oversight entities such as the Office of Research Oversight (ORO), Office of Inspector General (OIG), Food and Drug Administration (FDA), and others.
2. Because VA has not yet obtained an approved Records Control Schedule for facility research data, data collected in VA research studies must be maintained indefinitely by the VA facility until an applicable Schedule is approved by the National Archives and Records Administration (NARA).[[8]](#footnote-8)

**Disclosure of Data Under HIPAA Authorization**

1. A subject’s authorization under HIPAA permits VA to disclose the subject’s protected health information (PHI) to an academic affiliate or other non-VA collaborator for the research described in the authorization.[[9]](#footnote-9)
2. Disclosure of the subject’s PHI under a subject’s HIPAA authorization constitutes the first scenario addressed in the *Working Group* report. A Data Use Agreement (DUA) is **not** required under this scenario.[[10]](#footnote-10),[[11]](#footnote-11)
3. HIPAA authorization and informed consent requirements apply, respectively, to all VA protected health information (PHI) and individually identifiable private information used and/or disclosed for research. The HIPAA authorization and informed consent requirements apply whether the information was collected for clinical purposes or for research, and extend to the use of purely clinical data in research “control” or “comparison” groups.
4. The HIPAA authorization, informed consent document, study protocol, and (where applicable) Cooperative Research and Development Agreement (CRADA) underlying such disclosures must be **consistent** about the purpose of the disclosure and the data to be disclosed. The informed consent document (and process) must provide sufficient information for prospective subjects to make a genuinely informed decision regarding participation and must include all of the required elements.[[12]](#footnote-12),[[13]](#footnote-13)
5. The informed consent document and HIPAA authorization must address any anticipated use and/or disclosure of the data for future research (i.e., research outside the study for which the data were collected).
6. A research data repository[[14]](#footnote-14) must be established if use and/or disclosure of the data by VA for future research is anticipated.

**Data Ownership and Information Security**

1. When VA research data are disclosed to an academic affiliate or other non-VA collaborator under legally effective informed consent and a valid HIPAA authorization (per Item #6 above), VA must retain a complete record (i.e., original or copy) of the disclosed data (per Item #1 and Item #2 above). The **retained record** is owned by VA, and remains subject to VA information security requirements (see Items #12 and #13 below).
2. Once in the possession of the recipient under this scenario, VA may no longer be able to control the **disclosed copy** of the data or enforce VA information security requirements.[[15]](#footnote-15)
3. The second scenario described in the *Working Group* report[[16]](#footnote-16) involves disclosures outside VA of individually identifiable research data where legally effective informed consent and/or a valid HIPAA authorization are lacking.[[17]](#footnote-17) ORO strongly recommends consulting ORD, the VHA Privacy Office, and Regional Counsel prior to any such disclosures.
4. VA information security requirements apply to **all** research data **owned** by VA.[[18]](#footnote-18)
5. If maintained electronically, **VA-owned** research data containing VA Sensitive Information (VASI) **must** reside on VA-owned equipment (e.g., VA servers within the VA protected environment) unless (a) a waiver for the data to reside on other (non-VA) equipment (e.g., academic affiliate servers) has been approved in writing by VA’s Chief Information Officer (CIO);[[19]](#footnote-19) (b) a valid Memorandum of Understanding / System Interconnection Agreement (MOU/SIA) has been approved;[[20]](#footnote-20) or (c) where appropriate, a valid contract that includes VA’s security clause and appropriate security requirements has been established to permit alternate arrangements for the storage of VA-owned data.[[21]](#footnote-21)
6. ORO strongly recommends consulting the Office of General Counsel or Regional Counsel, the VHA Privacy Office, and the Office of Research and Development (ORD) when there may be doubt about the requirements for the disclosure of research data.

**Investigators Holding Dual Appointments**

1. When investigators hold dual appointments at a VA facility and the facility’s academic affiliate (or other non-VA entity), it is necessary to **separate** and **document** their activities as **VA employees on VA time** versus their activities as **affiliate/collaborator employees on affiliate/collaborator time**.
2. Documentation should clarify (i) VA duties, (ii) VA duty locations, (iii) VA tours of duty or time allocations, (iv) issues related to data ownership, and (v) research information protection and data security requirements. VA research should be conducted on VA time. Clarity regarding data ownership and data security issues will be difficult to establish without written documentation.
3. **Separation of VA activities/research** **from affiliate/collaborator activities/research is critical** when dual appointment investigators wish to conduct studies that require combining VA data with affiliate/collaborator data.

**Combining Data Collected at a VA Site and an Affiliate/Collaborator Site**

1. The following conditions apply to protocols in which research data are collected, used, and disclosed under legally effective informed consent and a valid HIPAA authorization.
2. When a study will **combine** data collected at both a VA site and an affiliate/collaborator site, the study should be implemented as a **multi-site** study with one of the sites serving as the “Coordinating Center.” The Coordinating Center site will receive the data disclosed by the other site and combine the data as needed for analysis.
3. Data collection must take place at the VA site and at the affiliate/collaborator site as **separate** **activities** that can be clearly distinguished.[[22]](#footnote-22)
4. If the affiliate/collaborator’s IRB serves as the VA’s IRB of Record, the IRB must either (i) approve two separate “protocols” (one VA “protocol” and one affiliate/collaborator “protocol”),[[23]](#footnote-23) ***or*** (ii) approve a single “protocol” in which the activities constituting **VA research** can be clearly **separated** from the activities constituting the **affiliate/collaborator research**.[[24]](#footnote-24) In either case, the VA **R&DC** may **only** approve the **VA research**.

c. HIPAA authorizations, informed consent documents, and study protocols for both sites must make clear that (i) resultant data are to be used in a multi-site study that combines VA data with affiliate/collaborator data; and (ii) the data are to be disclosed to the Coordinating Center site where the data will be combined and analyzed for the study.

1. Where the Coordinating Center holding the “combined” data set is located at the VA site, the VA research described in the “protocol” approved by the VA IRB and R&DC must include (i) the interaction/intervention and data collection activities at the VA site, and (ii) the activities of the Coordinating Center in receiving and combining the data from the affiliate/collaborator site.
2. Where the Coordinating Center holding the “combined” data set is located at the affiliate/collaborator site, a dual appointment investigator should not use the combined data set while on VA time unless approved as an “off-site” VA research activity in consultation with ORD and Regional Counsel.[[25]](#footnote-25)
1. This interim guidance does not apply to any other type of disclosure. ORO is providing this guidance because there is a pressing need for clear procedures for disclosing data to VA’s academic affiliates and other research partners, pending resolution of several key policy issues. For example: (i) The Veterans Health Administration (VHA) proposed Records Control Schedule for facility research data has yet to be approved by the National Archives and Records Administration (NARA), so such records must currently be retained indefinitely. (ii) Information security policies in VA Handbook 6500 are currently under review, and modifications may ensue. (iii) Advances in technology make it likely that VA information storage and retrieval may eventually be centralized, making much of the guidance provided here obsolete. ORO will maintain close contact with the Office of Information and Technology (OI&T), the Office of General Counsel (OGC), the VHA Privacy Office, and the VHA Office of Research and Development (ORD) to ensure that this interim guidance is updated promptly as policy evolves. [↑](#footnote-ref-1)
2. This guidance supersedes previous ORO guidance on this matter, including its memoranda dated May 14, 2009 (*Further Guidance on ORO Implementation of VA Handbook 6500 §6c(4)(J));* May 29, 2008 *(Compliance Oversight Procedures for Use and Storage of VA Sensitive Information);* and February 2, 2009 *(Further Guidance).* [↑](#footnote-ref-2)
3. <https://www.aamc.org/download/138118/data/va_report.pdf.pdf> [↑](#footnote-ref-3)
4. Title 5 United States Code Section 552a (5 USC 552a) [↑](#footnote-ref-4)
5. Title 38 Code of Federal Regulations Section 1.550-1.559 (38 CFR 1.550-1.559), 38 USC 5701, 38 USC 7332 [↑](#footnote-ref-5)
6. 44 USC 3301 [↑](#footnote-ref-6)
7. 36 CFR 1228.42(B) [↑](#footnote-ref-7)
8. When an applicable Records Control Schedule is approved and implemented, VHA will promulgate the Schedule, and Paragraph 2 of this guidance will no longer be in effect. [↑](#footnote-ref-8)
9. HIPAA at 45 CFR 164.508. Per HIPAA at 45 CFR 164.514(a)&(b), an authorization is not required for disclosure of de-identified information. [↑](#footnote-ref-9)
10. The Flow Chart in Appendix 1 (page 8) of the *Working Group* report describes disclosure of PHI pursuant to a request from an academic affiliate, presumably for use in non-VA research conducted by the affiliate. It is ORO’s understanding, pending formal clarification in VA policy, that disclosure of PHI for “collaborative” research (involving both VA data and affiliate data) under a HIPAA authorization would likewise not require a DUA (or other similar written agreement). [↑](#footnote-ref-10)
11. Likewise, a DUA (or other similar written agreement) is not required for disclosure of de-identified information. [↑](#footnote-ref-11)
12. Federal Policy (Common Rule) for the Protection of Human Subjects at 38 CFR 16.116(a). [↑](#footnote-ref-12)
13. VHA Handbook 1200.05 §§31 & 32, as applicable. [↑](#footnote-ref-13)
14. VHA Handbook 1200.12. [↑](#footnote-ref-14)
15. This reflects ORO’s interim guidance (based on the *Working Group* report), pending formal clarification in VA policy that the *Working Group* report can be extended to “collaborative” research (involving both VA data and affiliate data) as indicated in footnote 10 (above). It is ORO’s understanding that disclosure of data under a HIPAA authorization does not necessarily, in and of itself, transfer ownership of the disclosed information to the recipient. However, if a DUA is not employed under this scenario, it may be difficult for VA to exert ownership of the disclosed copy of the data. Thus, it would appear that a DUA (or contract per Item #13) that clearly specifies ownership of the disclosed data is advisable if VA wishes to exercise ownership or control of research data disclosed to an academic affiliate or other non-VA collaborator. ORO recommends that any DUA executed for disclosure of research data for any purpose outside VA clearly address (a) the permitted uses of the data by the recipient; (b) the data ownership status of all copies of the disclosed data; and (c) applicable data storage and information protection requirements. [↑](#footnote-ref-15)
16. The Flow Chart in Appendix 1 (page 8) of the *Working Group* report describes such disclosure of PHI pursuant to a request from an academic affiliate. [↑](#footnote-ref-16)
17. Per VHA Handbook 1605.1 §13.b(1)(c), a disclosure pursuant to a request from an affiliate/collaborator for individually identifiable VA data for use in non-VA research requires approval from the Under Secretary for Health in addition to a DUA and waivers of informed consent and HIPAA authorization requirements. For disclosures of identifiable information for “collaborative” research, an applicable Privacy Act System of Records Routine Use must also exist in order to disclose individuals’ information without their consent. [↑](#footnote-ref-17)
18. VA Directive 6500 and its implementing VA Handbooks. [↑](#footnote-ref-18)
19. The waiver process assures the CIO that appropriate security controls are established on the recipient’s system per VA Handbook 6500 §6.c(4)(j). [↑](#footnote-ref-19)
20. VA Handbook 6500 §6.a(13). [↑](#footnote-ref-20)
21. Metadata (e.g., information on how the data were collected, measurement, level of accuracy, data ownership, etc.) may be required about the data exchanged or transferred where the data are in electronic form and it is determined that the data can be released to third parties (e.g., in response to a Freedom of Information Act request). [↑](#footnote-ref-21)
22. The VA research must be approved by the VA Institutional Review Board (IRB) and the VA Research and Development Committee (R&DC), and the affiliate/collaborator research must be approved by the affiliate/collaborator IRB. The VA R&DC may not approve the affiliate/collaborator research. [↑](#footnote-ref-22)
23. Research facilities exercise considerable latitude in developing administrative procedures to manage their research projects; thus, the definition of “protocol” may vary from site to site. The intent here is not to require specific administrative procedures but to ensure that VA research is clearly distinguished from affiliate/collaborator research, so that (i) VA activities can be separated from non-VA activities, and (ii) the VA R&DC only approves the VA research. [↑](#footnote-ref-23)
24. It is recommended that informed consent documents and HIPAA authorizations for all existing “protocols” be amended to ensure separation of VA versus non-VA research at applicable continuing reviews occurring after December 31, 2011. Facilities should also ensure such separation in all new “protocols” reviewed after that date.  In addition to informed consent documents and HIPAA authorizations, relevant areas of separation for new protocols may include recruitment procedures, strategies, advertisements; research related procedures; data collection, storage, uses, disclosures; researchers and study team members; VA clinics, units, labs, locations; VA ISO and PO reviews; etc. It may also be necessary to develop an MOU (or other written agreement) between the VA and the non-VA entity, and/or corresponding standard operating procedures (SOPs), to ensure that the VA R&DC approves only the VA research. [↑](#footnote-ref-24)
25. Data ownership and information security requirements are unclear under this scenario. [↑](#footnote-ref-25)