

VA Data Security and Privacy: Frequently Asked Questions

RESEARCH DATA/SENSITIVE INFORMATION:

Q: What constitutes sensitive information?

A: According to VA Directive 6504, "VA sensitive information" is defined as data that require protection due to the risk of harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information. The term includes (1) information whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, (2) proprietary information, (3) records about individuals requiring protection under various confidentiality provisions such as the Privacy Act and the HIPAA Privacy Rule, and (4) information that can be withheld under the Freedom of Information Act (FOIA).

Q: Is de-identified health information sensitive information?

A: Health information de-identified in accordance with VHA Handbook 1605.1 Appendix B would not be considered sensitive information.

Q: Is de-identified qualitative data (focus group transcripts/recordings, interviews) considered sensitive information?

A: Verbatim written transcripts and audio or video recordings should be treated as sensitive information.

Q: What is the difference between de-identified data and a limited data set? Would a limited data set be considered sensitive information?

A: De-identified data is health information that does not identify an individual and there is not reasonable basis to believe that the information can be used to identify an individual. The information must not contain any of the following: (1) names/initials, (2) all geographic subdivisions, smaller than a state, (3) all elements of dates except the year and all ages over 89, (4) telephone numbers, (5) fax numbers, (6) e-mail addresses, (7) social security numbers (real or scrambled), (8) medical record numbers, (9) health plan beneficiary numbers, (10) account numbers, (11) certificate or license numbers, (12) vehicle identifiers and license plate numbers, (13) Device identifiers, (14) URLs, (15) IP addresses, (16) biometric identifiers, including finger and voice prints, (17) full-face photographs and any other comparable images, and (18) any other unique identifying number, characteristic or code, unless otherwise permitted by the Privacy rule for re-identification. Along with removing the 18 identifiers, HIPAA also states that for the information to be considered de-identified, the entity does not have actual knowledge that the remaining information could be used alone or in combination with other information to identify the individual who is the subject of the information

A limited data set is not de-identified information or data. It may contain: (1) city, state, zip code, (2) elements of dates and other numbers, (3) characteristics or codes not listed as direct identifiers, (4) identifiable information such as scrambled SSN's. Storage of limited data sets in

a non-secure environment (containing dates and limited geographical information only) may be allowed with a properly executed data use agreement.

Local policy has determined that limited data sets are not to be considered sensitive information at this time.

TRAINING:

Q: What online training modules must be completed to fulfill VA Research Data Security and Privacy Requirements?

A: The VA requires that all staff involved in VA research including (but not limited to) all VA Research Office personnel, investigators, study coordinators, research assistants, trainees such as house officers and students, administrative support staff (including secretaries and clerks), and members of the IRB and Research & Development Committee complete three training modules through the VALO website:

- 1) VA Research Data Security and Privacy Training,
- 2) Cybersecurity Training
- 3) Privacy Training.

Note: Personnel includes compensated and without compensation (WOC) employees, and IPAs.

Q: Are individuals listed on the VAPHS Staff Form as exempt required to complete these training modules?

A: No.

CERTIFICATION (SUBMISSION OF APPENDICES C AND D OF THE FEBRUARY 6th 2007 MEMORANDUM):

Q: When does the PI have to complete the certification?

A: All VAPHS Principal Investigators must submit Appendix C (Data Security Checklist for Principal Investigators) and Appendix D (Principal Investigator's Certification: Storage & Security of VA Research Information) at the time of any new protocol submission, and annually, by April 15th, for each active research protocol.

Q: I am not involved with Human Subjects Research, must I still complete Appendix C & D?

A: Yes. For accounting purposes, we are asking that all investigators submit Appendix C & D at the time of new study submission and annually by April 15th. For those studies that do not involve Human Subjects Research, you may simply indicate "Not applicable" on the forms.

OFF-SITE STORAGE/TRANSFER

Q: What is the procedure for asking permission to store VA data off-site?

A: Permission to remove data from a VA facility or VA system (which would include storing the data on a non-VA system) must be obtained from the PI's immediate supervisor, the ACOS/R&D, the ISO, and the Privacy Officer. The first step in the process would be to complete the Request for Approval of Off-Site Storage/Transfer of Research Data Form. Once completed, the form should be signed by the PI and his/her supervisor. Once those signatures have been obtained, the form can be forwarded to the IRB office, in conjunction with your new study submission or protocol modification/amendment. The submission will be reviewed to ensure that the protocol and consent adequately address data security and privacy issues. If necessary, this may include a physical inspection of the site where the data will reside in order to ensure that the non-VA site meets the same security requirements as a VA facility. Once all concerns have been resolved, the ISO, Privacy Officer, and ACOS/R&D will approve the request. Instances in which the concerns cannot be resolved will result in disapproval.

Q: If data is sent to a sponsor and the data was collected under an informed consent and HIPAA authorization do we need to get permission from our supervisor, the ACOS/R&D, the ISO and the Privacy Officer?

A: Yes. Local policy dictates that transfer or storage of all research data off-site is subject to approval. Your project will be reviewed to ensure that the protocol, consent, and the agreement with the sponsor adequately address data security issues. Furthermore, when the data is sent to the sponsor it must be transmitted in compliance with all VA requirements. While the data and all copies are in VA possession, all VA requirements must be met.

STORAGE DEVICES:

Q: May I use a personal thumb drive to store my research data?

A: The use of any personal storage devices at the VA is strictly prohibited.

Q: I would like to take my laptop off-site. Do I need permission to do so?

A: Yes. There are specific forms that must be completed in order to take equipment off-site. If you would like to take Government Furnished Equipment (i.e., VA or VAPHS Research Foundation purchased) off-site, you will need a Check-Out Sheet from the Research Office (Contact Nick Squeglia, AO/ACOS/R&D, at Nicholas.Squeglia@va.gov).