Frequently Asked Questions

The most current FAQs include all previous FAQs and any corrections or additions. New information, since the last update, is highlighted in blue. Each answer includes a creation date and a revision date if applicable.

RESEARCHDATA@VA.GOV:

Q: Why are you not accepting telephone questions?

A: The subject of this information security assessment touches upon the responsibilities of many VA offices. By putting your questions in writing, ORD, which is taking the lead in ensuring questions are answered, is able to get input from all concerned parties in answering your question.

To help us more quickly get your questions to the right experts we ask that you summarize your concern in the subject line of emails you send to RESEARCHDATA@VA.GOV. (Created 2/9/07)

What's Covered Under the Security and Privacy Review?

Q: Information security issues transcend research and extend to educational and clinical areas. Is VHA taking measures to oversee veterans' data that is shared with affiliates as part of educational and patient care?

A: Yes, VA is concerned and is taking measures to ensure all VA sensitive data including personal health information, remains secure. (Created 3/5/07)

Q: Are VA nonprofit research corporations covered under this security and privacy review?

A: Yes. This security and privacy review does concern the VA nonprofits, research supported by the nonprofits, their employees and any research data stored on nonprofit provided computers. (Created 3/2/07)

Q: Do the data requirements apply to data associated with studies open at the VA only because VA effort is used in the conduct of the study? That is to say there are no VA patients included and the study is not funded by the VA.

A: Your question does not provide enough information to venture an answer. Please discuss these issues directly with your local privacy officer and IRB. Ultimately your Medical Center Director is responsible for the protection of research data, working through the local Research and Development Committee. Data requirements apply to all research; the key is the presence of sensitive information.

We believe the best way to formulate this, and many similar questions we have received, is as follows**: "is there a risk to privacy or confidentiality here and, if so, how should we (VA) address it?"** (Created 2/14/07; Revised 2/16/06)

Q: Please clarify whether this is for research pertaining to only VA patient information or does it include basic science protocols, unrelated to VA patients?

A: All studies should complete the check list and certification forms indicating "**not applicable"** where appropriate for accountability and auditing purposes. (Created 2/14/07; Revised 3/2/07)

Q: My research does not require IRB committee approval. Do I need to complete the check list and certification forms?

A: All studies should complete the check list and certification forms indicating "not applicable" where appropriate. (Created 2/13/07)

Q: Our R&D program closed. We still have documents related to those projects. Does the PI need to complete the checklist and certification for these protocols?

A: No, only active protocols are covered under the memorandum. However, if any data relating to those projects is sensitive, it should be stored in a secure manner. (Created 2/13/07)

Q: I have a VA-funded research program with an approved off-site waiver that does NOT involve human subjects or human subject material. Do I need to complete the checklist and PI certification? How do I respond to Appendix C?

A: We recommend that all VA-funded research programs with approved off-site waivers complete the checklist. If the research does not involved human subjects or human subject materials, select N/A (not applicable) on Appendix C. All studies will complete the check list and certification forms indicating "not applicable" where appropriate in order to maintain accountability and auditing purposes for all VA funded research programs. (Created 2/13/07; Revised 3/2/07)

Q*: Not all research is under the supervision of the ACOS/R&D at a facility. Does this requirement apply to research where the researcher's supervisor is not at the facility where the program is 'housed'?*

A: Yes, all research regardless of supervisory channels must comply with this requirement. Examples include, but are not limited to, the MIRECCS, PADRECCS, GRECCS, any mental health or MS Center of Excellence, etc. These centers are encouraged to discuss this further with their direct reports in Patient Care Services. (Created 2/12/07)

Q: On the conference call it was stated that the protection of sensitive data applies to everyone: PIs, staff assistants, administrative staff, IRB and Research and Development (R&D) Committee members. However, only the PI has to fill out the certification checklist. Will there be forms that the rest will have to complete for the protection of sensitive data?

A: Under this initiative, the research **education** requirement will be for all research staff. The **certification** process is the responsibility of the PI for each research project. (Created 2/9/07; Revised 2/12/07)

Relations with Academic Affiliates and NIH:

Q: Is there any guidance on the status of Case Report Forms (CRFs) that have a study ID that includes the subject initials? For those industry sponsored studies that require CRFs to be sent to the sponsor, does the investigator need to obtain permission from 1) immediate supervisor, 2) ACOS/R&D, 3) VA Information Security Officer and 4) VA Privacy Officer prior to sending these forms?

A: If the subject has signed a written Informed Consent document and a HIPAA Authorization that permit release of data to the sponsor, this authorization would allow disclosure of individually-identifiable health information to the Sponsor or FDA, as indicated on the form, under the HIPAA Privacy Rule, Privacy Act and 38 USC 7332. However, it is the responsibility of the principal investigator, the ACOS and all VA Medical Center personnel involved in the chain of command to the Medical Center Director to ensure that the data is transferred in an appropriately secure manner. We expect that it should not be difficult to implement appropriate security measures within the matter of a few days in most cases.

Following transfer, any data that is continued to be maintained at the VA must comply with 6504 and other relevant VA policies. (Created 2/14/07)

Q: We are concerned that the security and privacy review may adversely affect key research efforts with our affiliates.

A: We realize that VA research is highly collaborative and that the new requirements imposed by VA directives and the February 6, 2007 memorandum could potentially impact those collaborations. We need to work together to keep the research mission going, but it's also critical to emphasize that securing sensitive research data is the principal objective.

VA leadership has already initiated dialogue with the academic community and other federal sponsors of research so that our respective efforts are aligned and synchronized. We also want to highlight that the Federal Information Protection Standards that form the basis of VA policy apply to all Federal contractors and may be part of the Terms and Conditions for specific federal grants.

We urge you to engage in dialogue with your university partners to ascertain whether specific shared data repositories are covered by the definition of sensitive data, and whether their current IT infrastructure is compliant with applicable VA standards. Some VA facilities have found it useful to establish a joint VA-affiliate "Research Information Security Workgroup" to address these issues on an ongoing basis.

Your local Information Security Officer (ISO) and Chief Information Officer (CIO) are the "go-to" persons for any concerns and questions concerning information security. If you have questions about whether data within a specific study are covered by the VA directives and memorandum, please email a detailed description to us at researchdata@va.gov. (Created 2/9/07)

Q: Our university affiliate is physically connected to the VA facility. Is this campus considered a location outside the local VA?

A: It depends on whether or not your local VA medical center director deems the University space as part of the medical center (i.e., if there is an agreement for shared space). If this is the case, the ISO and VA Chief of Police would need to certify that the space/equipment/data are compliant with the

requirements of this VA security and privacy review. If there is not an agreement for shared space with the University, it would be considered a separate non-VA location.

Federal Information Security Management Act (FISMA) requires all non-VA sites having government equipment and/or data must meet the same security requirements as a VA facility. Accordance with the Federal Information Security Management Act of 2002 (FISMA), which states in the relevant section:

> The head of each agency shall be responsible for providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of the agency. (H.R. 2458—51 section 3544).

(Created 2/9/07; Revised 2/12/07 and 3/2/07)

Q: I have an NIH grant that requires data sharing. Am I allowed to share those research data?

A: If the research data are not from human subjects, they may be shared. We are working with NIH to establish the ground rules for research involving human subjects. However, VA data may only be shared with outside entities, such as NIH, with appropriate legal authority, such as informed consent, as outlined in Federal privacy laws and regulations. Your facility Privacy Officer can provide assistance on determining if legal authority exists to disclose VA data. (Created 2/9/07; Revised 2/12/07)

VA Data at Non-VA Sites:

Q: I have a VA-owned laptop that has VA-approved encryption software and VPN software installed. This computer has identifiable information from human subjects. If I take this laptop to another site (such as a university) for collaborative work, may I connect to their network?

A: It depends on what type of connection is being made at the other work site and the security of the files on your laptop. If you are connecting to a local area network at the other work site that would allow others to have access to the files on your laptop, then that could possibly be a security breach issue if the permissions were not set properly on the files that contain patient identifiers. Since file permissions cannot be verified, the recommendation would be to not connect to any non-VA networks when using a computer that contains any protected VA data. The VAINOC@va.gov group can provide additional guidance regarding connectivity issues.

File permissions do not provide data security protection from a knowledgeable IT person. The laptop will be encrypted and only non-VA collaborative facilities meeting the VA security standards will be allowed to unencrypted these working files. Accordance with the Federal Information Security Management Act of 2002 (FISMA), which states in the relevant section:

> The head of each agency shall be responsible for providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of the agency. (H.R. 2458—51 section 3544).

(Created 2/12/07; Revised 3/2/07)

Q: What is the procedure for asking permission to store VA data at a non-VA site, and whose permission do I need?

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 your immediate supervisor, the ACOS/R&D, the ISO, and the Privacy Officer. No formal form or format for this request has been developed at this time.

Additionally, if Individually Identifiable Health Information is stored on a non-VA system, a Business Associated Agreement will probably need to be negotiated. Contact the VA Privacy Compliance Team for more information.

If any non-VA personnel could possibly have access to the data that is now stored on a non-VA system, they would have to complete all of the VA security requirements, which, at a minimum, would include taking the AIS Security Awareness training and Privacy training. Depending upon the level of access, a background investigation may also be warranted.

Federal Information Security Management Act (FISMA) requires all non-VA sites having government equipment and/or data must meet the same security requirements as a VA facility. If a non-VA facility does not meet these requirements, the data could acquire viruses, hacker attachment code, possible data download, release sensitive data to unauthorized entities, or possible destruction of the VA networks. Accordance with the Federal Information Security Management Act of 2002 (FISMA), which states in the relevant section:

> The head of each agency shall be responsible for providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of the agency. (H.R. 2458—51 section 3544).

(Created 2/12/07; Revised 3/2/07)

Research Sponsors:

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. No, if the approved protocol and the agreement with the sponsor addresses this issue. When the data is sent to the sponsor it must be transmitted in compliance with all VA requirements. In addition, while the data and all copies are in VA possession, all VA requirements must be meet. (Created 3/2/07)

Multicenter Research:

Q: Some researchers have remote access to FISMA encrypted VA servers on which their data is resident. Can they work remotely (VPSN) in this manner or is that considered removing data from "within VA?"

A: The issue of data encryption is accomplished via ONE VA VPN, however the equipment being used for access **will** be government furnished equipment (GFE); if it is a laptop, it must also be encrypted. (Created 2/16/07)

Q: Do researchers need the written permissions (supervisor, ACOS/R&D, ISO and Privacy Officer) to transfer data from one VA to another on a FISMA encrypted CD or FISMA encrypted computer? Does your response differ if the FISMA encrypted computer is personal property?

A: The encryption protocol must be FIPS 140-2 compliant, and any personal property that stores VA data must also meet all VA mandates for access controls and FIPS 130-2 encryption. In addition, the equipment must also conform to the VA's media sanitation requirements when no longer used for storing VA data.

If the VA data is being used outside the scope of the research study that it has been approved for, and/or for another purpose, then yes, permissions and/or Memorandums of Agreement will need to be completed or renegotiated. (Created 2/16/07)

Q: How should we ensure the security of research data that are submitted via a "workbench" website for a multicenter clinical trial?

A: We assume that either the data has been de-identified according to both the Common rule and HIPAA definitions, or that the patient has signed a HIPAA waiver of Authorization that permits transfer of Protected Health Information to the data coordinating center. The computer used should comply with all VA data security protocols and reside within the VA firewall, unless implementation of these protocols precludes transmission to the data center. If implementation of the VA security measures, investigators should work with OIT staff to develop an interface compatible with appropriate privacy protections, while continuing to transmit data using the current configuration. The need to protect the safety of veterans enrolled in clinical trials includes the need to develop secure solutions for transmitting data to data centers and sponsors. Investigators will work with OIT staff to develop an interface compatible with appropriate privacy protections, before transmitting data (Created 2/9/07; Revised 2/13/07, 2/14/07 and 3/2/07)

Q: In a multicenter research study who is responsible for cybersecurity?

A: In a multicenter research study, the PI (or Principal Proponent) is responsible for cybersecurity, along with the staff of the data coordinating center, and the site PI at any location where study data is collected.

The Cooperative Studies Program Coordinating Centers are working with OIT staff to assure that these systems are compliant with VA Directive 6504. (Created 2/9/07)

Sensitive Information:

Q: Is data derived from de-identified human cell lines, such as HeLa cells, considered VA-sensitive information?

A: VA-sensitive information is not generated from work on de-identified cell lines obtained from external resource centers such as the American Type Culture Collection or NIH-funded cell repositories. In addition, data derived from de-identified human tissue from the Cooperative Human

Tissue Network or other NIH-funded resource centers is not considered VA-sensitive information. (Created 2/16/07)

Q: What constitutes sensitive information?

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

Most results of VA research may be withheld from FOIA responses prior to publication, but not subsequently. Once published, this type of information is not considered "sensitive." (Created 2/9/07; Revised 2/12/07)

Animal Research:

Q: Should we consider anything that falls in USDA Category E as falling into the category of sensitive?

A: All decisions regarding sensitivity of animal research projects (including USDA Category E) are to be made at the local level and formulated from VA standards and polices for animal research projects. (Created 2/14/07; Revised 3/2/07)

Q: Can non-sensitive animal data be stored on non-VA computers?

A: Yes, it may be stored on non-VA computers as long as those computers are not connected to the VA intranet.
Non-VA computers can not be connected to a VA network. Federal Information Security Management Act (FISMA) requires all non-VA sites having government equipment and/or data must meet the same security requirements as a VA facility. If a non-VA facility does not meet these requirements, the data could acquire viruses, hacker attachment code, possible data download, release sensitive data to unauthorized entities, or possible destruction of the VA networks. Accordance with the Federal Information Security Management Act of 2002 (FISMA), which states in the relevant section:

> The head of each agency shall be responsible for providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of the agency. (H.R. 2458—51 section 3544).

(Created 2/13/07; Revised 3/2/07)

Q: Is certification required for animal research protocols?

A: No. This certification requirement refers to research protocols that require institutional review board (IRB) approval. Since animal research protocols do not require IRB approval, certification is not required for these protocols. All studies **will** complete the check list and certification forms indicating "**not applicable"** where appropriate in order to have accountability for all animal research protocols. (Created 2/9/07; Revised 2/14/07 and 3/2/07)

Q: Is there any animal research that does generate sensitive research information?

A: Yes, typically those projects provide for review by an outside entity prior to publication. They are difficult to define but are of a nature that both the investigators and facility director will be able to identify them and the need for enhanced data protection.
The investigators and facility director will identify all sensitive research information through the VA standards and policies governing this type of data for all VA facilities.
(Created 2/9/07; Revised 3/2/07)

Q: Are there any reasons why, or instances where, data on animal experiments should be encrypted?

A: There are at least two reasons: (1) to assure that, when the data are released to the public, they are put into context, and (2) to reinforce good data security practices among investigators.

Data requires protection due to the risk of harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information. The term includes information whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary information, records about individuals requiring protection under various confidentiality provisions such as the Privacy Act and the HIPAA Privacy Rule, and information that can be withheld under the Freedom of Information Act.
(Created 2/9/07; Revised 3/2/07)

Q: Please clarify or define the type of data collected during animal experimentation that would be considered "sensitive" for the purposes of the security requirements directive.

A: In most instances, data derived from sources other than human subjects would not be covered by VA Directive 6504 or the Feb 6 2007 memorandum.

However, certain circumstances might create the need to treat non-human subjects' data as if they were VA sensitive data. These circumstances are dictated by sponsor requirements or the nature of the protocol and usually will be apparent to the principal investigator or local research office. When in doubt, consult with the scientific program manager for the study sponsor, or the VA Chief Veterinary Medical Officer. VA standards and Policies dictate the parameters of sensitive data for the principal investigator or local research office.

We advise, in general, the practice of encrypting with a FIPS 140-2 certified encryption tool for all data stored on portable media such as laptops and all types of removable memory devices (e.g., USB devices, SD memory cards). (Created 2/9/07; Revised 2/16/07)

Medical Resident Research:

Q: Medical residents are required to complete a research project and many of them choose to study patients at the VA where much of their training is done. What are the privacy and data security requirements for this research?

A: Residents must obtain legal authority under Federal privacy laws and regulations to be able to use VA health information for research. The Privacy Officer can assist in ensuring the resident has met the appropriate privacy requirements before VA data is used for their research project. Residents may never have research information (even if de-identified) on a personal laptop, PDA, or USB drive, unless the resident has been granted permission from their supervisor, the privacy officer, ISO and the ACOS/R&D or research coordinator. Laptops or portable media used by residents for research must be encrypted and password protected. (Created 2/9/07; Revised 2/12/07)

HSR&D REAPs:

Q: We have personnel who cannot complete the cyber sessions scheduled for HSR&D REAPs. Can the online training be in lieu of the Cyber session?

A: Yes. The intent of the cyber sessions is to provide HSR&D REAP staff an early opportunity to complete the training requirement. The online course will take some time to produce and put on the web. A special 2007 Cyber Security Awareness course for researchers will soon be available through EES. (Created 2/14/07; Revised 2/15/07)

Q: We have a PI at our HSR&D REAP, but all of the data collection, storage and analysis is taking place at a non-REAP Site. Is the work at the non HSR&D REAP site(s) subject to the HSR&D REAP Security and Privacy Certification?

A: Yes. As the overall PI for the project, the investigator at your HSR&D REAP is ultimately responsible for the activities at the participating sites for this study. As such, even if no data is being collected, stored or analyzed at the REAP site, all sites participating in the study are subject to the requirements of the HSR&D REAP Security and Privacy Review/Certification with respect to this study.

Federal Information Security Management Act (FISMA) requires all non-VA sites having government equipment and/or data must meet the same security requirements as a VA facility. Accordance with the Federal Information Security Management Act of 2002 (FISMA), which states in the relevant section:

> The head of each agency shall be responsible for providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of the agency. (H.R. 2458—51 section 3544).

(Created 2/12/07; Revised 3/2/07)

Q: Is the HSR&D REAP responsible for the cyber security of QUERI activities taking place at the local facility where the REAP is located?

A: All HSR&D and QUERI activities at your facility are reportable through the REAP and, as such, are subject to the HSR&D REAP security and privacy review. (Created 2/9/07)

Q: When do investigators need to report to ORO and OHRP with regard to our current Security and Privacy Review?

A: The Information Security Assessment that the Office of Research and Development (ORD) is requiring at each VA research facility (including facilities with HSR&D REAPS) does not itself constitute a suspension reportable to ORO and OHRP.

However, if the Facility, through its Information Security Assessment or any other mechanism, identifies a problem that results in suspension of a study by the local IRB, that suspension should be reported promptly by the Facility Director to both the appropriate ORO Regional Office and OHRP. ORO Regional Offices are available to provide additional clarification, if needed. (Created 2/9/07)

Certification:

Q: In completing the checklist for a study where the patient has signed a consent and a HIPAA authorization for release of PHI is it acceptable to send study data in Case Report Forms to a sponsor or collaborating institution? In this situation, going by the checklist, some data would be stored outside of the VA. Should I check No for the first specific requirement and then get the appropriate approvals from my supervisor, the ACOS for R&D, the Privacy Officer and the ISO or does the fact that the patient has authorized the release of the information mean that I should check No or N/A?

A: You must be sure that the data "handling" while in the VA (including copies) and the transmission meet VA standards. The transfer of data to the sponsor must also follow what is in the approved protocol. Once the data are “delivered” to the sponsor under the terms of the research agreement, further approvals are not needed, assuming the veteran has signed a consent and HIPAA authorization. (Created 3/5/07)

Q: Does the Certification by Principal Investigators only apply to Active Protocols? Does the Certification apply to Continuing Review Protocols?

A: The certification applies to all protocols that are actively collecting, analyzing, or transmitting data, including new protocols and continuing review protocols. (Created 3/5/07)

Q: Appendix D, PIs Certification, does not bear the word “signature.” May this form be completed by typed entries in the blanks?

A: You may do so as long as it is understood that entry of the typed name constitutes an actual certification by the investigator. Be sure to keep the forms on file that the Medical Center Director has certified. (Created 2/9/07)

Computers:

Q: If you have individually identifiable data on your VA office desktop computer must the computer be encrypted?

A: Policy is currently silent on encrypting standalone PCs, so we have not mandated it yet (Exception: you should sanitize the hard drive if you are discarding the equipment).

ALL standalone PCs are required to be encrypted if it contains data which requires protection due to the risk of harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information. The term includes information whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary information, records about individuals requiring protection under various confidentiality provisions such as the Privacy Act and the HIPAA Privacy Rule, and information that can be withheld under the Freedom of Information Act.
(Created 2/16/07)

Q: We have researchers who were unable to obtain the approved FISMA encryption software through the VA and ended up purchasing it with grant funds from the non-profit. Will adequate software be made available to researchers to avoid additional purchases such as this?

A: OIT has assured us that software will be made available. Please contact your local IRM shop. All software being purchased and used on VA equipment must be the same products listed on the Authorized VA Software Listing.
(Created 2/16/07)

Q: When researchers leave the VA, they often take computer equipment that was purchased with their NIH grant with them. Will this situation be considered in the certification process?

A: No, this should be handled at the local level and should be included in the out-processing procedure. Equipment should be sanitized prior to leaving the VA. The local Property Officer will maintain a listing of all IT equipment (including grant purchased equipment) used in the facilities and the ISO will document that sanitization was has been completed on each component requiring sanitization prior to leaving the VA.
(Created 2/13/07; Revised 2/16/07)

Q: Is the purchase of software and hardware used to protect research assets to be done with patient care or research funds?

A: Neither, the purchase of software and hardware use to protect VA research assts must be made with IT funds. (Created 2/12/07)

Q: Can Mac computers be encrypted?

A: Yes, you can purchase them encrypted or purchase encryption software. Make sure that the software is FIPS 140-2 certified. All software purchased for VA usage will be items from the VA Authorized Software Listing.
(Created 2/12/07; Revised 3/2/07)

Q: Should encryption software be used on "embedded computers"? (Embedded computers, also referred to as "dedicated computers," are computational devices that are used to collect data from a scientific instrument and are "part and parcel" of that instrument.)

A. No. Use of encryption software on embedded computers may void the manufacturer's warranty or service agreements. In addition, it may cause these computers to malfunction. As a rule, embedded computers **will** not be used as general purpose computers. (Created 2/9/07; Revised 3/2/07)

VPN:

Q: Is there a limit to the number of VPN accounts that can be requested by an individual medical center to support improved compliance with data storage requirements?

A: No, there isn't a limit to the number of VPN accounts that can be requested, if their need is justified. Please e-mail VAINOC@va.gov for additional guidance regarding VPN accounts. (Created 2/12/07)

Clinical Labs:

Q: What are the requirements for reference labs that process samples?

A: Reference labs generally handle samples for a short time. All data must be coded. (Created 2/12/07)

Scientific Presentations and Publications:

Q: Our researchers are getting ready to make presentations at a scientific meeting and wonder if they can take their de-identified data with them for this purpose. Does de-identified data require signatures from the supervisory, ACOS/R&D, ISO and Privacy Officer?

A: If the data has been de-identified it is by definition **Not** VA sensitive information, and therefore would not require signatures. This does not alleviate the requirement to protect sensitive data that is not associated with personally identifiable information such as, contractual information or proprietary information that may be associated with others. (Created 2/16/07)

Hard Copy Data:

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. The key with sensitive, non-electronic information is to use appropriate physical security in its storage, transit and ultimate destruction. (Created 3/5/07)

Q: What is the guidance for hard copy data stored in off-site space associated with an approved off-site waiver?

A: All VA-funded research that involves VA sensitive data, electronic or otherwise, should be in compliance with current VA policies for data storage and security requirements. Your local Privacy

Officer should be able to provide specific guidelines for storage and security of hard copies. For example, hard copies should be stored in locked cabinets with restricted access etc. For studies that do not involve VA sensitive data, while it is not required, we recommend that the VA medical center maintain a checklist and certification forms for all studies with an approved off-site waiver, indicating "not applicable" where appropriate. (Created 2/16/07)

VA Research Data Security and Privacy Training:

Q: Does the New VA Research Data Security and Privacy Training replace the Cyber Security and VHA Privacy Training, or is it in addition to these prior training courses?

A: It is in addition to the Cyber Security and VHA Privacy Training required for all VA employees. (Created 3/4/07)

Removable Media:

Q: In our research we work on protocols, worksheet templates, etc. frequently using our thumb drives and laptops. Does this mean we have to have "specific permissions" to put our grant applications and protocols on USB thumb drives so that we can work on them on non-VA servers?

A: Yes, permission must be obtained to put the data on any portable media and remove it from VA. Also, see the new VA Directive 6601 dated 2/27/07 on use of removable storage devices. If VA sensitive data is on the PCs then all VA requirements apply. (Created 3/5/07)