June 4, 2007

Key Points Related to Privacy & IT Security

These Key Points have been designed to replace the Frequently Asked Questions (FAQs) document that has been posted on the ORD website. These points have been distilled from the FAQs, questions asked by field facilities, discussions with the VA Office of Information &Technology (OI&T), the VHA Privacy Office, other VA and VHA offices, and recently published policies. Information that is no longer applicable has been deleted. As additional Key Points are developed they will be added to this document. Note:

The Key Points have been arranged within seven major topic areas:

1. Key Definitions
2. Sensitive Information
3. Storage of Data and Storage Media
4. Human Subjects Research
5. Database Research
6. Animal Research
7. Other Key Points

1. Key Definitions

- **Covered research studies.** Research studies covered by the data security requirements include all studies approved by the Research and Development (R&D) Committee regardless of funding source. *See the definition of sensitive data to assist in determining if the data generated by the covered studies require further protections.*

- **Certification and Accreditation (security).** As stated on the (National Institute of Standards and Technology (NIST) web-site (http://www.NIST.gov): "Federal Information Security Act) (FISMA) requires that all Federal agencies develop, document, and implement a program to provide information security for the information and information systems that support the operations and assets the agency including those provided or managed by another agency, contractor, or other sources." A Security Certification and Accreditation is a mechanism used to indicate that the system meets specific security requirements and that there is an ongoing risk management process. *Note: OI&T will be developing information/guidance to assist in understanding the standards that must be met whenever VA sensitive data are stored outside of VA.*

- **Data transfer agreement (DTA).** A DTA may also be called a data use agreement (DUA). A DTA is required when data are transferred from one VA investigator or VA facility to another VA investigator or VA facility if the transfer is **not** within the "scope" of an approved protocol (from one protocol site to another). If the data are going to be transferred outside the scope of a protocol to a non-VA investigator or non-VA institution, the facility's Privacy Officer must be contacted prior to the transfer and approve the release of the data. *Note: Transfer of data to the sponsor of a clinical trial or to coordinating centers including those for the Cooperative Studies Program, does **not** require a DTA. See also Data Use Agreement.*

- **Data Use Agreement (DUA).** Under HIPAA a DUA is a document that is developed between a covered entity (e.g., all of VHA is considered one covered entity) and the recipient of a limited data set. It describes how the data will be used and disclosed; explains what safeguards will be in place to prevent other uses or disclosures of the information; holds the recipient to the standards, restriction and conditions stated in the DUA; and prohibits the recipient from identifying the individual from whom the information was derived or contact those individuals. Although DUA is a specific term used within the HIPAA regulations, it is sometimes used in place of the term. *See also Limited Data Set and Data Transfer Agreement.*

- **De-identified data.** Data that meet the HIPAA (45 CFR 164.514(b), VHA Handbook 1605.1) and Common Rule (38 CFR 16) definition of de-identified. For HIPAA this requires the removal of all 18 "HIPAA identifiers". HIPAA does include provisions for statistically determining a data set de-identified (45 CFR 164.514(b)(1)). .

- **Encryption.** Encryption is the process of changing or converting data/information so that a code or some type of key is required to read the data/information. *See FIPS, next.*

- **Federal Information Processing Standards (FIPS).** FIPS is put out by NIST and sets forth requirements for both computer hardware and software. If a manufacturer's certification of hardware or software is validated to the FIPS standards, then the hardware or software is said to meet the current government standards for sensitive but unclassified information. FIPS 140-2 is the current standard for encryption software. Publications on NIST standards may be found at: http://www.itl.nist.gov/fipspubs/. The following are some of the FIPS publications relevant to security of VA information:

    - 140-2 "Security Requirements for Cryptographic Modules" May 25, 2001 (Supersedes FIPS PUB 140-1, 1994 January 11). This document describes the cryptography standards for both hardware and software components. A list of FIPS 140-2 validated products may be found at: http://csrc.nist.gov/cryptval/140-2.htm.

    - 199 "Standards for Security Categorization of Federal Information and Information Systems," 2004 February

    - 200 "Minimum Security Requirements for Federal Information and Information Systems," 2006 March

- **FISMA.** The Federal Information Security Act in Title III of the E-Government Act of 2002. It addresses the security of information and information systems that support the operations and assets of an agency. FISMA requires that all Federal agencies develop, document, and implement an agency-wide programs to provide for this security. Those operations provided or managed by another agency, a contractor, or other sources are also covered.

- **Limited Data Set.** This is a dataset that contains Private Health Information (PHI) that excludes 16 categories of direct identifiers. A limited data set may be used or disclosed without obtaining either an individual's authorization or a waiver of authorization granted by an Institutional Review Board (IRB) or Privacy Board. The limited data set may be used only for the following purposes: research, public health, or health care operations. A limited data set may contain some direct identifiers, therefore, research conducted using the data may constitute human subjects research.

- **NIST.** The National Institute of Standards and Technology (NIST) is a non-regulatory Federal agency within the U.S. Department of Commerce's Technology Administration. NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life. The Information Technology Laboratory within NIST develops standards for computer security including those for encryption that meets Federal requirements.

- **Principal Investigator (PI).** For purposes of VA policies and guidance on privacy requirements and IT security, the term PI refers to the VA investigator responsible for the research at a particular VA facility/site and not an "overall" PI that may be located at another VA site or a non-VA site. PI for the purposes of this guidance is the VA site PI. *Note: For CSP studies the assigned CSP Coordinating Center has the primary responsibility for ensuring compliance with all data transfer policies.*

- **Risk Assessment.** Risk can be described as the probability or chance that an incident can occur that will cause harm. A risk assessment is a process that allows one to characterize the harm (loss of privacy, identity theft), identify who will be harmed (subjects, investigators, VA), the magnitude of the harm, and the probability that the incident will occur. It also involves identifying the steps that should be taken to prevent the incident or if the incident cannot be prevented, minimize the harm that may occur. NIST Special Publication 800-12: An introduction to Computer Security – The NIST Handbook describes steps for conducting a risk assessment. It also includes a case study on assessing and mitigating the risks to a computer system.

2. Sensitive Information

- **Sensitive Information.** Also see sensitive research data. VA sensitive information is all Department data, on any storage media or in any form or format, 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 specifically 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.

    - Examples of VA sensitive information include the following: individually-identifiable medical, benefits, and personnel information; financial, budgetary, research, quality assurance, confidential commercial, critical infrastructure, investigatory, and law enforcement information; information that is confidential and privileged in litigation such as information protected by the deliberative process privilege, attorney work-product privilege, and the attorney-client privilege; and other information which, if released, could result in violation of law or harm or unfairness to any individual or group, or could adversely affect the national interest or the conduct of federal programs.

- *Clarification: The definition of Sensitive Information does not included ALL Department data. It does include Department data that require protection due to risk of harm that could results 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.*

- **Sensitive research data.** All research data that contain information about human subjects AND have not been de-identified are considered sensitive research data.

  - Other research data including de-identified human subjects data, animal data, and data developed during other types of studies may be sensitive depending on what information is contained within the data, the topic of the research, and its impact of the VA.

  - An evaluation must be completed to identify any VA sensitive information that may be developed during the research. If VA sensitive information will be developed a risk assessment for impact of a data breach should be conducted. Based on this risk assessment appropriate privacy and security safeguards must be put in place. Involve the local Privacy Officer and Information Security Officer (ISO) to assist in developing such safeguards.

3. Storage of Data & Storage Media

- **CD ROM/DVD Media Protection.** CD-ROM/DVD that **contains sensitive information** (see definition below) must be protected with a VA approved encryption solution that is FIPS 140-2 validated. *For examples of FIPS 140-2 validated software, please see either NIST web site (http://csrc.nist.gov/cryptval/) or speak with your ISO*

- **Laptop computers.** All VA owned laptop computers must be encrypted using FIPS 140-2 validated encryption software. In addition, VA sensitive information may not reside on non-VA laptops or other portable media unless the appropriate permissions have been obtained. Policies that address these issues include: VA Directive 6504, 6600, and 6601. Laptops computers that are not owned by the VA that contain VA Protected Information must be equipped with, and use, A VA-approved antivirus software and personal (host-based) firewall that is configured with a VA-approved configuration. The antivirus software and firewall must be updated regularly and run continuously. VA-approved encryption software must also be used, i.e, the encryption software must be FIPS-140-2 validated. *See encryption.*

- **USB devices and other removable storage media.** VA Directive 6601 requires that all VA employees, contractors, and others having access to and storing VA information must:

  - Have permission from a supervisor and ISO to use Universal Serial BUS (USB) or other removable storage media. If these devices are used, they must contain protective features that have the approval of the local senior OI&T official.

- Prior to removing VA sensitive information from the VA, have written approval from their respective VA supervisor and ISO.

- Use encryption.

- Obtain OI&T approval of the protections for the sensitive data prior to removing them from the VA.

- **Other types of storage.**

  - Audio recordings: Most audio recordings of research subjects are considered to be identifiable unless the voice print has been altered in such a way as to make it impossible to match the voice print with the subject's voice print and no identifying information is present on the recording. Audio recordings that are considered identifiable must be protected per VA policy.

  - Paper records: Paper copies or original documents containing sensitive information must be secured in such a way as to prevent non-authorized persons from accessing them. When no longer required they should be shredded using a cross-cut shredder.

  - Video recordings: Sensitive information stored on video media must be secured per VA policy.

- **Storage of data at non-VA locations.** Research data that are collected when the IRB has waived the requirement for both the informed consent and HIPAA authorization may not be stored outside of the VA unless permissions have been obtained from at minimum, the facility ISO, and the ACOS/R&D. *Note: Others permissions may be required such as the Facility Director, the facility's Chief Information Officer, the Privacy Officer, and your supervisor. Many of the current guidance documents and policies related to this issue currently being revised. Your facility's ISO should be contacted for the latest requirements.*

4. Human Subjects Research

- **Collection of research data.** Research data containing subject identifiers and PHI may be collected a) directly from a research subject after an informed consent and HIPAA authorization has been obtained or b) from pre-existing databases or third parties after the IRB has waived the requirement for informed consent and HIPAA authorization.

  - Informed Consents and HIPAA Authorizations obtained. The signed Informed Consent and HIPAA Authorization that are obtained prior to collecting research data must describe in a meaningful way who will have access to the subject's data; where it will be sent, and what part of the data will be sent to another facility, a non-VA entity, and/or the research sponsor. The transfer/transmission of the research data outside the VA must occur in accordance with VA policy and the approved protocol.

  - Waiver of informed consent and HIPAA authorization by an IRB. Patients identifiers and PHI collected under this mechanism must remain within the VA and securely stored

as required by VA policy. Storage within the VA should be on a secure VA server. The data may not be transferred/transmitted outside the VA unless permissions have been obtained as required by VA Directive 6504 and 6601.

- **Multi-site clinical trials.** The VA PI (site PI) is responsible for all aspects of the protocol conducted at his/her VA site including privacy and security of data. In addition, if data are transferred out of the VA, the transmission and storage of data at the non-VA site must meet VA requirements. *See also Transfer of clinical trial data and Principal Investigator.*

- **Privacy review.** All new protocols should be reviewed by a knowledgeable person to verify that there is compliance with all applicable statutes, regulations and policies related to privacy. This person may include, but is not limited to, the Privacy Officer, the ISO, research compliance officer, IRB administrator, and/or others. The VHA Privacy Office website (http://vaww.vhaco.va.gov/privacy/) contains a number of useful tools and Fact Sheets to assist with this review.

- **Specimens sent to non-VA laboratories.** When required, human biological specimens may be sent to non-VA reference laboratories as required by an approved protocol. The accompanying data should not contain any of the HIPAA identifiers unless there is a compelling justification, and the data should remain there for the shortest time possible. A Data Transfer Agreement (DTA) outlining use of the data should be developed. Permission from ORD must be obtained to "bank" the specimen at that location. See Data Transfer Agreement (DTA).

- **Transfer of clinical trial data.** Research data that have been collected under a signed informed consent and HIPAA authorization as appropriate, may be transferred to the sponsor or coordinating center per the approved protocol. The data must be transfer/transmitted per VA policy but the VA is not required to review or evaluate the sponsor's computer system for security. A DTA is not required.

- **Transfer of identifiable research data when the IRB has waived informed consent and HIPAA authorization.** When the IRB has waived the requirement to obtain an informed consent and has waived the requirement to obtain a HIPAA authorization transfer and/or storage of the data outside the VA may only occur after consultation with the ACOS/R&D, your supervisor, your facility's ISO, and your facility's Privacy Officer.

    - There must be a security evaluation of the non-VA computer or non-VA server where the information will be stored and a risk assessment must be done to evaluate the potential for loss, theft or inadvertent disclosure of the information.

    - Required permissions must be obtained prior to transfer as required by applicable VA and VHA policy and guidance.

    - If approved has been obtained to store the data on a non-VA computer or non-VA server, transfer of the data must be in compliance with all applicable policies and guidance.

- **Transfer of identifiable data at the request of a non-VA investigator or institution.** Requests from non-VA investigators or non-VA institutions for VA data must be sent to your facility's Privacy Officer. The release of the data is controlled by the Privacy Act,

VA's System of Records, HIPAA, VHA Handbook 1605.1, and other privacy related regulations and policies. VA investigators cannot release the data without the appropriate permissions from the Privacy Officer.

5. Database Research

- **Aggregate data.** Data that are combined from multiple individuals or from several measurements are not usually considered identifiable data nor is it usually considered to be sensitive data. The sensitivity determination must be made for each specific research project and it must be made based on the VA definition of sensitive data.

- **Data from human subjects.** Database research may involve identifiable data or de-identified data.

- **De-identified data.** Data that have been de-identified by HIPAA and the Common Rule criteria are usually not considered sensitive data and as such the harm that would result from risk level of a data breach would be much lower and therefore the risk level would be lower. A risk assessment of the specific data that are being used should be performed to ensure they would not be considered sensitive based on the impact on an institution, groups of individuals, or other factors. The data should stay within the VA whenever possible and if taken out of the VA there must be an appropriate justification.

- **Data NOT derived from human subjects.** These data are usually not considered sensitive data and, as such, the risk level of a data breach would be lower but one must evaluate the content of the data, however a risk assessment of the specific data that are being used should be performed to ensure they are not sensitive based on the impact on an institution, groups of individuals, or other factors. The data should stay within the VA whenever possible, and if taken out of the VA there must be an appropriate justification.

- **Identifiable data.** The storage and security of identifiable research data must follow that for clinical trials and human subjects research in section 4. Human Subjects Research. This type of research is considered human subjects research and falls under the Common Rule (38 CFR 16).

6. Animal Studies

- **Animal data.** In most instances, animal research does not generate sensitive data, however, a risk assessment must be done to determine if there is a potential for harm from unauthorized use or release of the data. If at all possible the data should remain on VA computers.

7. Other Key Points

- **Business Associate Agreements (BAA).** A BAA is normally not required for research purposes because research is not one of the functions or activities regulated by HIPAA (treatment, payment, or health care operations). Therefore when data are transferred outside of the VA as required by the approved protocol, a BAA is not required of the receiving entity. *See Nonprofit Corporations for an exception to this.*

- **Educational requirement.** 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 must have current information security training as specified by ORD. Personnel include compensated and without compensation (WOC) employees, and IPAs. Local facilities must maintain documentation that training requirements have been met. The VA Research Data Security & Privacy course is available through the VA Learning Online (VALO) Campus or the Learning Management System (LMS). This course was posted March 15, 2007, and must be completed no later than June 12, 2007, for all staff. Newly hired staff should complete training as soon as possible but definitely prior to beginning any VA research activity or any access to sensitive information. This course will be an annual requirement and may be found at: http://www.research.va.gov/resources/data-security/training.cfm.

- **Nonprofit Corporations (NPC).** A VA NPC must follow *all* VA and VHA requirements on privacy, IT security, and educational requirements when it has possession of VA sensitive information or its employees are engaged in research. *Note: If research subject information goes to the NPC, the NPC needs a BAA with VHA unless the informed consent and HIPAA authorization specifically state that the NPC will receive the information.*

- **Presentations and Publications.** If data have been de-identified by HIPAA and the Common Rule criteria permissions are not required prior to incorporating the data into presentations or publications unless they are considered sensitive or if the research subject gives written permission to allow the use of his/her identifying information. *See De-identified data and sensitive data also.*

- **SSNs and names requested by sponsor.** Normally, veteran names and SSNs should not be sent to pharmaceutical industry sponsors. The case report forms should instead use a code that would not identify the individual study subject.

    - If the study sponsor indicates that there is a specific regulatory requirement for including names and SSNs, this must be clearly explained by the sponsor and the regulatory requirement must be verified by either Regional Counsel OR the VHA Privacy Office.

    - If there are reasons based on the scientific protocol for including names and SSNs (e.g., studies that may utilize the National Death Index, Medicare claims, or other databases requiring name and SSN for data linkage) then the IRB and the R&D Committee must carefully weigh this request and consider the benefits that may be derived by the research subjects and the risks that are inherent in sending this information outside VA. The

protocol must be scientifically sound and there should be evidence of adequate provisions to protect subject identifiers.

- If the IRB does approve a protocol that would allow the names and SSNs to be sent to the sponsor, the informed consent and the HIPAA authorization must clearly state that the individual's medical information includes name and SSN. They must also be worded to convey the risks and the benefits to the subject, as well as the measures that will be taken to protect the security of the data. Additionally, the informed consent should specify that neither the VA investigator nor the Veterans Health Administration will have any control over how that information will be used after the case report forms are transferred to the study sponsor.

Limited Data Sets

The following identifiers must be removed from a data set containing health information for the data set to be considered a limited data set. The identifiers may either apply to the individual, the individual's relatives, the individual's employer, or the individual's household members.

(1) Names

(2) Postal address other than town, city, state, and ZIP code

(3) Telephone numbers

(4) Fax numbers

(5) SSNs

(6) Medical Record number

(7) Health plan beneficiary numbers

(8) Account numbers

(9) Certificate/license numbers

(10) Vehicle identifiers and serial numbers including license plate numbers

(11) Device identifiers & serial numbers

(12) Web universal resource locators (URLs)

(14) Internet protocol (IP) address

(15) Biometric identifiers, including fingerprints & voice prints

(16) Full-face photographic images and any comparable images

Note: A limited data set may be considered human subjects research depending on the type of data it contains.

HIPAA Identifiers

These 18 identifiers must be removed to consider the data de-identified. The identifiers may either apply to the individual, the individual's relatives, the individual's employer, or the individual's household members.

(1) Names

(2) All geographic subdivisions smaller than a state, except for the initial three digits of the zip code if the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people

(3) All elements of dates except year for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older.

(4) Telephone numbers

(5) Fax numbers

(6) E-mail addresses

(7) Social security numbers

(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 and serial numbers

(14) URLs

(15) Internet Protocol (IP) addresses

(16) Biometric identifiers including fingerprints and voiceprints

(17) Full-face photographs and any comparable images

(18) Any other unique, identifying characteristic or code, except as permitted for re-identification in the Privacy Rule

Note: In addition, the covered entity must also have no actual knowledge that the remaining information could be used alone or in combination with other information to identify the person who is the subject of the information.