Text for Special ORD Field Hotline Call
Tuesday, February 6, 2007
2:00 PM, ET

Good afternoon.   This is Joel Kupersmith, Chief Research & Development Officer, along with Joe Williams, Assistant Deputy Under Secretary for Health Operations and Management; Tom Puglisi, Chief Officer, Office of Research Oversight; and Arnie Claudio, Director for Oversight and Compliance from the Office of Information Technology.

You have received an electronic Memorandum from Mr. Feeley and me about a new initiative called “Certification by Principal Investigators: Security Requirements for VA Research Information.” Essentially this initiates a Security and Privacy Review.

The purpose of this call is:

1. To provide some background
2. To begin to review with you what this initiative entails, and
3. To review what will be required of you.

As you know, the Department of Veterans Affairs is committed to protecting sensitive information including veterans’ personal identifiers and health information. All of us at the VA – whether we are managers, researchers or administrators - are responsible for protecting our veterans’ confidentiality and personal information. If we don’t maintain the trust of the veterans we serve, we won’t be able to continue to conduct high quality health services and clinical research. In fact we won’t be able to conduct research at all.

We all need to remember that it is a privilege to be involved in VA Research. This privilege, however, comes with many responsibilities. One of the most important is to ensure that ALL VA research information is secure.

Another important responsibility is that we are familiar with, and operate in compliance with, all applicable regulations and policies related to privacy, confidentiality, and the storage and security of research data.

Recent events both inside and outside the VA have highlighted the potential vulnerability of sensitive information, including patient data in research studies.

Over the past few months we have received information and training about the standards for information security and privacy. We have also implemented many new requirements for information security. You have risen to the occasion and worked hard to implement these new measures. I want to congratulate you on your efforts to date.

However, we think it is critical that we take time now to document that we have done all we possibly can to safeguard research information.

For that reason, we are implementing a Security and Privacy Review. This consists of new training requirement and a process of certification including a project-by-project certification checklist that will encompass all VA research. The focus of this initiative will be on VA research data storage and security. It will include ensuring that each VA facility performing research has appropriate policies and procedures in place for research data storage and security, and that those policies and procedures are being implemented.

To these ends, this Security and Privacy Review is being initiated.A memorandum with instructions in the form of attachments has been sent by e-mail, signed by Mr. Feeley and myself, to all VA Medical Center and VISN Offices. We are requiring the following:

- That the Associate Chief of Staff for Research and Development (ACOS/R&D) or the Research Coordinator at each VA facility that conducts research convey this memo and its attachments to all staff involved in research, including all investigators, research assistants, administrative support staff, and members of the Research and Development Committee and Institutional Review Board. Local leaders must emphasize the importance of the requirements within the memo.

- By April 15, 2007, Principal Investigators are responsible for submitting a completed certification checklist found in Appendix C of the memorandum sent today. This checklist must be completed for each of their protocols and submitted to the Research Office at the local VA facility. Each research project at the facility will need to be reviewed for compliance with the requirements. The ACOS/R&D or Research Coordinator will be responsible for confirming the PIs' checklist information.

- A special training program, targeted to all staff involved in research, is being developed, that will emphasize the particular points within the memo, and must be completed no later than 90 days after it is available.

- By May 1, 2007, all ACOS/R&Ds or Research Coordinators will have ensured that all PIs have submitted their certification checklists, and will have forwarded written certification to the Medical Center Director that all local PIs have met the certification requirement.

- By May 15, 2007, all Medical Center Directors will have certified to their VISN Directors that all local PIs have met the certification requirements related to storage and security of research information. These certifications will be maintained in the VISN Director's files.

- By May 21, 2007, VISN Directors will have notified their VISN Support Team that they have received certifications from each of their facilities that all PIs have completed certification checklists

This certification process must be completed annually with the same due dates each year.

What are we looking for?

The appendices to the Memorandum you will receive will contain definitions of key terms and information on the regulations and policies. I want to take a moment to review just SOME of the kinds of information security requirements we are talking about.

- Research data generated by VA investigators during the conduct of VA-approved research is owned by the VA. Therefore, investigators' use and storage of these data must meet all Federal standards, including VA and VHA policies. For your convenience, we have posted a list of links to all this information on the ORD website, www.research.va.gov.

- VA research data may NOT be stored outside the VA unless the storage site meets VA standards, and permissions have been obtained from the person's supervisor, the ACOS/R&D, the Privacy Officer, and the ISO. This includes storage on non-VA computer systems, servers, desk top computers located outside the VA, laptops, or other portable media.

- Data transfer to a non-VA computer system, server or site CANNOT occur until AFTER the required permissions have been obtained. Also, the transfer must be in compliance with requirements found in VA Directives 6500 and 6504.

- When VA data are stored on a non-VA system, the system must meet all requirements set forth in the Federal Information Security Act (FISMA) including the required Certification and Accreditation of the system.

- Data must be encrypted according to current VA requirements AND password protected with only authorized individuals having access to the data. This holds true when they are stored on VA laptops, or on non-VA laptops OR desktops.

- ***Identifiable*** data on research subjects, including veterans names, addresses, and Social Security Numbers (whether real or scrambled) may only be stored within the VA and on VA servers. Remember HIPAA requires that 18 specific identifiers plus any other information that may be used to identity the subject, or the subject's family, employer, or household members must be removed for the data to be considered completely "de-identified."

- If the data are coded, the key to linking the code with these identifiers must also be stored within the VA, but not with the coded data.

- Beginning immediately, all new protocols that include the collection, use and/or storage of research information must specify who will have access to the data and how the data will be secured. If copies of the data will be placed on laptops or portable media, the protocol must also include a discussion of the security measures for these media. For existing active protocols, this information will be confirmed at each continuing review.

The commitment to guarding VA sensitive information includes protecting ALL information collected for research purposes. It is important to remember that research information can be sensitive even if it doesn't involve human subjects – for example, research involving animals or data from the evaluation of clinical programs.

I recognize that this certification process will mean a lot of work for everyone but it is critical to maintaining the trust of the veterans we serve.

As you know, the field of information security is evolving rapidly as new technologies emerge and new threats are identified. For that reason, the steps we are taking today are just the beginning. Please work with us to protect VA research data security and patient confidentiality. We must do everything in our power to protect our veterans and the sacred trust research participants place in us. Your efforts will not only help ensure their rights and welfare are protected, but they will also help ensure the future of VA Research.

In closing, we want to let you know how we will help you through this:

1. First, we have set up a dedicated email address, ***RESEARCHDATA@VA.GOV***, for your questions. We ask that questions be routed through the local Research Office so we can handle them more efficiently. Your questions will be answered as soon as possible.

2. As questions come in, we will post frequently asked questions or FAQs on the ORD website mentioned earlier –www.research.va.gov. We also will periodically circulate updates by email.

3. We will have conference calls approximately every 2 weeks, or more often if needed, to provide updates and give you a chance to ask questions.

We realize that many of you would like to review the memorandum first and get back to us with questions, and that's okay. Remember, the email address for questions related to the research security and privacy review is ***RESEARCHDATA@VA.GOV***.

I know that this will be a challenge for all of us in the coming weeks. Thank you again for your commitment to keeping veterans' information secure and for all the work you do.