Text for Special REAP Data Security Call
Tuesday, February 6, 2007
4:00 PM, ET

Good afternoon. This is Joel Kupersmith, Chief Research & Development Officer, along with Bill Feeley, Deputy Under Secretary for Health Operations and Management, Tom Puglisi, Chief Officer, Office of Research Oversight, and Arnie Claudio, Director for Oversight and Compliance, VA Office of Information Technology.

Earlier today, you received an electronic Memorandum from Mr. Feeley and me about a new initiative called "Certification by Principal Investigators: Security Requirements for VA Research Information." Additionally, at 2 pm today, a conference call was held with the VA research community describing the requirements of that Memorandum.

The purpose of this call is:

1. To go over what this new initiative means for Health Services Research and Development Research Enhancement Award Programs.
2. To describe the ***requirement*** for REAPs to complete in the next 30 days a security and privacy review of all projects.
3. To inform you that further data collection, data transfer, or data analysis must be deferred until after the certification checklist has been completed, verified by the ACOS, and approved by the Medical Center Director.
4. To describe the independent assessment process that will be conducted by teams from the VA Office of Information and Technology to ensure that the needed security measures described in the initiative are in place, and to identify any other opportunities to improve data security and privacy.

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.

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.

A recent event involving one of the HSR&D REAP sites has highlighted just how vulnerable patient data in research studies can be if appropriate protections are not in place. We are using the opportunity from recent "sentinel events" as a teaching moment for all of VA research, and are paying special attention to HSR&D REAP programs, to ensure their data are secure.

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. In addition, for the 7 sites that have HSR&D REAPs, we also want to implement, with help from the VA Office of Information and Technology, a special process of on-site assessment of data security and privacy measures.

As mentioned on the earlier call today, we are implementing for **all VA research** a new training requirement and a process of certification including a project-by-project certification checklist. 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.

For HSR&D REAPS, we are requiring that the certification checklist and special, research-specific training, be completed within 30 days. We know that is a very aggressive timetable, but it is needed to reduce the likelihood that a data loss similar to what happened earlier at one of the REAP sites not occur again.

Please note that in the memorandum sent by e-mail to all VA Medical Center and VISN Offices, we have required:

- 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. ***We ask that REAP leadership and Medical Center leadership at each of the REAP sites convey this information immediately to all local REAP investigators as well as any collaborators and co-investigators for any of your projects, regardless of site.***

- By March 8, all REAP 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 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, and will be made available at the earliest possible time. ***We ask that all REAP staff complete this training no later than March 8, 2007.***

- By March 12, 2007, all Medical Center Directors will have certified to their VISN Directors that all of their REAP projects have met the certification requirements and that all REAP investigators have completed targeted research security training. Your VISN Support Team should also be notified at that time.

Please note that, afterwards, REAP sites and ALL VA investigators will need to complete this certification process annually using the due dates announced in the earlier call today.

What are we looking for from you?

- We are asking that, over the next 30 days, you focus your activities on the review of all studies (active and closed) in which there are databases, data files, or other data collections. Because of the importance of this initiative, we ask that further data collection, data transfer, or data analysis be deferred until after the certification checklist is completed and approved by the ACOS for R&D and the Medical Center Director. This can be done on a project-by-project basis.

- Exceptions to the requirement to pause all data collection, transfer, or analysis activities occurring at REAPs may be made in certain instances with the approval of local leadership. We expect medical centers and VISNs will continue ongoing operational and data analysis activities that are intended to improve the timeliness of VA patient care and assure that each veteran continues to receive the highest quality of healthcare. Medical Center and VISN Directors have the ultimate authority to determine which activities are required to meet these operational imperatives.

- All REAP sites are required to complete an inventory of all studies (active and inactive) and list on a specific form, to be provided, all the particular data collections, data elements, storage characteristics, and security measures. This inventory sheet will form the basis for completing the certification checklist, and will assist the OI&T assessment teams when they do site verification visits. Appropriate action must be taken immediately for data elements or files that do not meet requirements.

- In addition, you will need to inventory all data collections and repositories *not* associated with a specific research study. The same security standards apply to ALL data collections.

- As you complete your inventory of studies and data collections, you may find redundant copies of data. While keeping in mind requirements for data retention and backup, unnecessary copies and files must be erased, overwritten, and/or destroyed according to VA requirements and the VA media sanitization directive.

Your information security officer will be able to assist you in securing this data and ensuring that it can be erased, sanitized, or destroyed according to VA requirements.

- For your convenience, the specific requirements, standards, and policies have been posted on the ORD website, www.research.va.gov.

- Please note that 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. If the data collection inventory identifies such instances, you must take immediate action to have them returned to reside within the VA firewall. 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.

- 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.

- After the Medical Center Director has approved all studies at a given REAP, a team from the Office of Information & Technology will visit to perform an on site assessment. Please note, this is a follow-up visit to you in fulfilling these requirements. We have the commitment of OI&T that those visits will be made with all due speed in order to assure that all research activities may resume quickly at your site.

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.

We 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. The process of re-establishing

trust, and getting your systems secure to allow resumption of data collection and use, is in your hands.

As you know, the field of information security is evolving rapidly as new technologies emerge and new threats are identified. 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 about every 2 weeks, or more often if needed, to provide updates and give you a chance to ask questions.

That's all the information we have for today. Now it's your turn to ask questions. We may not be able to answer all your questions today but will make every effort to get back to you as soon as possible.

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.