SFVAHCS Research Office guidance on remote consent, data collection, and video communications (living document)

Obtaining signed informed consent and HIPAA authorization:

At the present time, we are not aware of a readily available remote method of obtaining signed informed consent and HIPAA authorization electronically. UCSF allows DocuSign as an e-signature; however, this is not approved for signing VA consent documents.

- If the research does not have a waiver of documentation of informed consent (i.e., signed consent), VA subjects or their Legally Authorized Representative (LAR) must sign the consent form by hand.
- If the research does not have a waiver of signed HIPAA authorization, VA subjects or their LAR must sign the HIPAA authorization by hand.

Note: use of an LAR is determined by the IRB; not a matter of convenience.

You can now send encrypted VA email using Azure Rights Management Services (RMS) to external email addresses (e.g., Gmail) with the VA consent and HIPAA forms as attachments. The subject must be able to print the forms and sign by hand.

Given that in-person consent is currently prohibited in most cases, here are some options to consider for obtaining the hand-signed documents:

Option 1: the subject could scan/photograph each page of the signed documents and email the images back to the encrypted VA email or send via the MyHealtheVet secure messaging system. **This is the preferred method.**

Option 2: you can use video communication technologies that would allow the subject to display the signed documents on their camera, and then the study team could take screen shots of each page. This method should only be used if option 1 is not possible and if the study team is using government furnished equipment. More on video communication technologies is included below.

For either option, the digitized, signed versions must be downloaded to the VA network. There is no requirement to print hard copies. VHA accepts a legible image of a signed authorization the same as the original. Remember that the VA Research Compliance Officer is still required to audit all signed VA consent documents, but this can be done with digitized versions.

More guidance on the use of encrypted VA email and MyHealtheVet are included below.

Data collection:

VA research data can be collected electronically using external (i.e., outside of the VA network) systems. However, there is a requirement is that only copies of VA data can exist on external networks. The original long-term data must reside within the VA-protected environment, unless you have a signed waiver.

External data collection systems:

You should always first pursue internal VA systems or VA-approved external systems for remote data collection (e.g., VA REDCap). If those solutions are not feasible, we recommend the following secure, HIPAA-compliant systems accessible via UCSF MyAccess:

- UCSF REDCap: https://myresearch.ucsf.edu/redcap
- UCSF Qualtrics: https://it.ucsf.edu/services/qualtrics-web-surveys

Before choosing an external system, please do your due diligence to research the information security standards. We recommend that you document this for your records. Also, if you are obtaining signed VA HIPAA authorization, the external entity must be named in the Disclosure section.

Data storage:

If you use an external system for remote data collection, you must download and store a full set of the original data on the VA network. The full VA research dataset stored on the VA network will be considered the original data. The VA research data stored on external systems will be considered a copy. You can also store copies of de-identified data on external systems such as UCSF Box, etc. If you wish to store copies of individually identifiable health information on external systems, the legal entity hosting the system must be named on the VA HIPAA authorization.

Use of video communication technologies:

Please see the attached VA memorandum regarding use of video communication technologies. To summarize, we have been granted some temporary flexibility to use external technologies.

VA Video Connect (VVC) is a VA-approved video communication technology, so you should explore this option first. Chrome is the preferred browser to use for VVC.

If VVC does not suit your needs, external technologies such as Apple FaceTime, Facebook Messenger video chat, Google Hangouts video, Skype, and WhatsApp can be used. Be sure that all possible security protections are used/enabled such as entry passwords, especially if using Zoom. Here is UCSF's guidance on using Zoom: https://it.ucsf.edu/news/recommended-security-settings-zoom

In addition, this memorandum authorizes VHA personnel to use personally owned equipment (POE) in the absence of government furnished equipment (GFE). Do not use a personal phone to send text messages or emails regarding study visits.

Please keep in mind that this flexibility is only in effect for the duration of the national emergency and could be reversed sooner.

IMPORTANT NOTE: Any changes to the process for obtaining and documenting informed consent, data collection methods, and use of video communication technologies must be approved by the IRB prior to implementation.

April 15, 2020

Link to VA ORD Policy and Guidance page for human research:
https://www.research.va.gov/resources/policies/human_research.cfm

Direct link to VHA Directive 1200.05:
https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=8171

Links to guidance on encrypted VA email using RMS:
FAQs:
https://vaww.portal2.va.gov/sites/AIP/_layouts/15/WopiFrame2.aspx?sourcedoc=/sites/AIP/Shared%20Documents/Azure%20RMS%20Frequently%20Asked%20Questions.docx&action=default

User's guide:
https://vaww.portal2.va.gov/sites/AIP/_layouts/15/WopiFrame2.aspx?sourcedoc=/sites/AIP/Shared%20Documents/Azure%20RMS%20User%20Guide.doc&action=default

Additional guidance on sending encrypted VA email using RMS:

There are a few extra steps that external users will need to take to open encrypted VA emails using RMS. Therefore, before the first encrypted email is sent, we recommend that you send a very limited, generic message with written instructions using unencrypted email.

The initial email could say something like:

Hello SFVA patient/research participant/potential research participant,

We are conducting a research project that you may be interested in/have expressed interest in/etc. We will provide further information about the project via a separate encrypted email. Please review the attached instructions/instructions below (if embedded within the text) on how to open and respond to the encrypted email, or feel free to call us at _____ to talk you through it over the phone.

Thank you,

Name

SFVAHCS

You can send a test encrypted VA email to your personal/non-UCSF email and then right up the steps. Do not test with a UCSF email because there are no additional steps to open VA to UCSF emails using RMS encryption.

Other helpful links:

Guidance for VA Researchers on the Use of My HealtheVet Secure Messaging

FDA Guidance on Conduct of Clinical Trials of Medical Products during COVID-19 Pandemic

April 15, 2020

ORD COVID-19 SharePoint site which includes:

- FAQs Regarding COVID-19 Impacts on Research
- ORD-ORPPE April 6 2020 Human Subject Protection Issues Related to COVID-19