SUBJECT: Privacy and Confidentiality of Research Data

1. PURPOSE:

This SOP establishes procedures to protect the rights of individual research participants and ensure the confidentiality of research data.

2. DEFINITIONS:

ACOS/R: Associate Chief of Staff for Research
HIPAA: Health Insurance Portability and Accountability Act of 1996
IRB: Institutional Review Board
PHI: Protected Health Information
PII: Personally Identifiable Information
PI: Principal Investigator
PO: Privacy Officer
R&D: Research and Development
VHA: Veterans Health Administration

3. OVERVIEW:

It is the responsibility of all VA researchers and staff to be familiar with and to comply with existing policies, procedures, and directives regarding the protection of human subjects in research and the use and disclosure of individually identifiable information.

4. PROCEDURES:

a) **Privacy Training Requirements:** All research personnel within the facility must obtain annual privacy training in accordance with applicable requirements and VHA privacy.

b) **Privacy Review Process for All Human Subjects Studies:** The Privacy Officer and Information Security Officer will review the proposed human studies materials prior IRB review and inform the IRB of their findings. Written documentation of deficiencies will be conveyed by the IRB to investigators.

c) **Approval to Conduct Human Studies Research:** To approve research, the IRB must determine that there are adequate provisions to protect the privacy of subjects and the confidentiality of data.

d) **Investigator Responsibilities:** If the research data is to be collected under an informed consent, the informed consent under which the data were collected must include the possible options for disposition of the data. All privacy and confidentiality issues must be addressed in the protocol and reviewed by the Privacy Offer; an information security plan must be developed and reviewed by the Information Security Officer. The investigator must obtain HIPAA authorization for the use and disclosure of the subject's PHI, or obtain an IRB-approved waiver of HIPAA authorization unless other legal authority exists.

e) **Approval for Access to PHI/PII:** IRB approval for the study of data, documents, records, or pathological specimens where the subjects are identified, without documentation of informed consent and authorization, will require that the subject's interests are adequately protected and the importance of the research justifies the invasion of privacy.

f) **Access to VA Records after IRB Approval:** Persons not employed by the VA can only access medical and other VA records within the restriction of the Federal Privacy Act and other statutes.

g) **Contractor/Vendor Identification:** All contractors must wear issued contractor PIV Cards while working within the Medical Center. Vendors must wear issued Vendor badges identifying them while they are working within the Medical Center.

h) **Clinical Trial Monitors:**

   i) Identification: Clinical Trial Monitors must report to the Research Office to register as visitors, and wear issued Visitor badges while on site.

   ii) Access to Medical Records: Two methods for viewing a study subject's electronic medical record are permitted:

      a. *Limited Read-Only Access to Selected Data:* Study subjects who have consented to participate in the clinical trial and signed the study's HIPAA Authorization will be established as a clinical patient group within CPRS. Permissions will be set to allow the monitor to have read-only access to those records. The monitor is required to sign the National Rules of Behavior document and complete VA Information Security Awareness and VHA Privacy Policy training before CPRS access is granted and annually thereafter. The monitor must also provide their social security number, which will be used as their unique identifier. The monitor's SSN will be purged from CPRS at the end of each session.

      b. *VA Employee Driver:* An authorized member of the study team accesses the system with the monitor watching and shows the monitor only the information that the monitor needs and is authorized to see for the specific trial.

i) **Email and Encryption:** All electronic messages containing sensitive information and/or information that must be protected in accordance with the Privacy Act of 1974 or the Health Insurance Portability and Accountability Act (HIPAA) must be encrypted before transmitting.

j) **Electronic Communications**: The subject line of email and VistA messages cannot contain PHI/PII.

k) **Research Record Storage:** All temporary and permanent Federal records must be stored in such a manner that would: (a) prevent them from being changed or destroyed; (b) ensure they are retrievable; (c) ensure they are "readable"; and (d) secure them from unauthorized access. Electronic Federal records should be maintained on VA server. Working copies of electronic Federal records may be copied onto other media but once finalized or changed need to be copied back onto the VA server if they differ from the file that was originally downloaded to the removable media. Refer to Minneapolis Research Service SOP R&D-016 "Research Data Requirements" for details on data storage guidelines.

l) **Data Management:** Transmission and transfer of identifiable data must be performed in accordance with VA security policies. Electronic access to identifiable data in a research data repository must be controlled through appropriate access controls, such as usernames and passwords, in accordance with VA security policies.

m) **Data Destruction:** All identifiable data used and maintained as part of a research protocol must be retained or stored for the period of time stated in the applicable Privacy Act System of Records notice, Records Control Schedule (RCS) 10-1, and VA policy. Identifiable

information may not be destroyed except with appropriate destruction authority. Refer to Minneapolis Research Service SOP R&D-016 "Research Data Requirements" for details on retention guidelines.

5. REFERENCES:

VA Handbook 6500 "Risk Management Framework for VA Information Systems VA Information Security Program" (24 February 2021)

VHA Directive 1200.05 "Requirements for the Protection of Human Subjects in Research" (07 January 2019)

VHA Handbook 1200.12 "Use of Data and Data Repositories in VHA Research" (09 March 2009)

VHA Directive 1605 "VHA Privacy Program" (01 September 2017)

VHA Directive 1605.01 "Privacy and Release of Information" (24 July 2023)

VHA Handbook 1605.04 "Notice of Privacy Practices" (12 February 2024)

MVAHCS Human Research Protection Program Standard Operating Procedures

Minneapolis Research Service SOP R&D-004 "MVAHCS Investigator Responsibilities" (07 January 2025)

MVAHCS SOP Management of Information Policy MCP IM-02M: Privacy Policy (25 September 2020)

MVAHCS SOP Management of Environment of Care Policy MCP EC-01G: Environment of Care (01 August 2022)

Guidance on Implementation of Approved Methods for Clinical Trial Monitor Access – Memorandum from Under Secretary for Health for Operations and Management (07 June 2010)

The Common Rule (38 CFR Part 16)

The Privacy Act of 1974 (5 U.S.C. § 552a)

Health Insurance Portability and Accountability Act of 1996 (HIPAA) (Public Law 104-191)

VHA Records Control Schedule RCS 10-1 (02 November 2017)

6. ATTACHMENTS:

VHA Privacy Office "Privacy Fact Sheet: Use of Individually Identifiable Information in Microsoft Office Applications" (May 2017)

VHA Office of Research & Development "Draft Guidance on the Use of Electronic Mail and Electronic Text Messaging for Recruiting and Communicating with VA Subjects in VA Research" (28 July 2018)

7. **R&D COMMITTEE APPROVAL:** 07 January 2025

8. **RECISSIONS**: Minneapolis Research Service SOP R&D-003 "Privacy and Confidentiality of Research Data" (04 June 2019).

9. **EXPIRATION DATE:** N/A

10. **FOLLOW-UP RESPONSIBILITY:** Research and Development (R&D) Committee

Privacy Fact Sheet

May 2017

Use of Individually Identifiable Information in Microsoft Office Applications

This fact sheet provides guidance to the field on when it is appropriate to include individually identifiable information (III) and/or protected health information (PHI) when using Microsoft Office Outlook Calendar, Microsoft Outlook E-mail, Microsoft Lync, and Text Messaging. Electronic mail (e-mail) and information messaging applications and systems are used as outlined in VA policy (VA Directive 6301, VA Directive 6500, and VA Handbook 6500). These types of messages should never contain Individually Identifiable Information (III), unless the authentication mechanisms have been secured appropriately. Authenticated mechanisms approved for use in VA is Public Key Infrastructure (PKI) for external and internal messages and Rights Management Service (RMS) for internal VA messages. See below when Outlook may be used to send one-way VHA communications without encryption.

Are there identifiers that are acceptable to be sent via outlook email without encryption?
Office of General Counsel (OGC) indicated that last four numbers of the Social Security Number (SSN) and first initial of the last name are not identifiable by itself. However, when you add any other individually identifiable information or health information that has not been de-identified in accordance with VHA Directive 1605.01 you may no longer send this alphanumeric code via Outlook without encryption.

For example you **can** send the following messages in Outlook without encryption:

"Please look at the co-payment bill for A#### as I think there is a mistake on the bill."

“The list of employees that will be involved in the Environmental Rounds from my Service are as follows:

Mary Smith, John Jones, Sue Brown”

However, you **cannot** send the following message in Outlook without encryption:

" On January 1, 2007 A#### had an appointment in the Cardiology Clinic. The visit for that appointment was coded wrong. The diagnoses should be CHF not cardiovascular disease."

What is considered individually identifiable or personally identifiable and should not be sent in outlook email unless encrypted?

Sensitive information per VA definition:

* Name (employee names are acceptable)
* Address
* Social Security Number
* Names of Relatives
* Other information regarding relatives
* Telephone/Fax/Other Numbers
* Photographs or Physical Presence; or
* Geographic Destination Smaller than a State.

NOTE: See VHA Directive 1605.01, Appendix A for additional information on HIPAA de-identification of data.

What is acceptable to place in the subject line of an outlook email message? The first initial of the last name and last four of the social security number by itself is not considered individually identifiable and therefore can be included in the subject line. Any non-identifiable information can be placed in the subject line.

NOTE: Subject lines are not able to be encrypted.

Is patient-provider communication that contains PHI or III acceptable over email?
No. The VA has not given permission to communicate personally-identifiable or any protected health information with patients/Veterans from or to private electronic mail accounts such as AOL.com, Verizon.com, Yahoo.com, or any .com address even if the patient/Veteran initiates the electronic communication. If initiated by the patient/Veteran and the message contains III or PHI, VA cannot respond back and must call or write the patient/Veteran. Secure Messaging (SM) within My Health***e***Vet, VA's Personal Health Record (PHR), is being used nationally. Secure Messaging allows for secure, two-way electronic communication between patients and members of their health care team.

NOTE: Secure Messaging through My Health***e***Vet is **not** considered email. Secure Messaging (SM) is web-based, encrypted communication between patients and health professionals. For patients, SM through My Health***e***Vet offers convenient access to healthcare team members for non-urgent issues. For clinical staff, SM provides a personal and efficient way to communicate virtually with patients. Patients must complete My Health***e***Vet In-Person Authentication, visit the Secure Messaging page and Opt In (agree to terms of use). For more information, contact the My Health***e***Vet Coordinator in your VA facility and/or visit Secure Messaging Through My HealtheVet

Can VA employees text a Veteran?

Yes, as long as there is no PII or PHI in the text as we are following the same guidelines that we would for email (see VA Handbook 6500). You cannot mention specific locations of appointments and any additional information except as follows:

Reminder: You have an upcoming appointment at the Tampa VAMC later this week in Buidling ### Rm #. Please call 321-123-3213 to confirm your appointment time or if you have any questions.

A date and time of an appointment by itself is okay, but it should never be combined with a facility name or location or a clinic name or location. Doing so makes it PII/PHI.

Reminder: You have an upcoming appointment with VA on August 16, 2017 at 0830 am. Please call 321-123-3213 to confirm your appointment or if you have any questions .

While date and time of an appointment is a Patient Identifier, it must be combined with where and what in order to be identifiable.

Can a provider get an authorization from a Veteran to allow VA to send III and PHI through email
No. Unfortunately, an authorization would not solve the problem as a Veteran cannot give permission for VA to ignore a security policy or requirement. Security policy states that VA sensitive personal information cannot be sent via email unless secured (e.g. encryption).

Is there a difference in the security of messages on outlook when sending intra-agency vs. inter-agency?
No. There is no difference in the security of sending messages on Outlook within your facility or outside your facility to another VA. Encryption requirements equally apply

Is it acceptable to include PHI in the Outlook Calendar?

No. Calendar controls were not designed to secure Personally Identifiable information or Protected Health Information. The security controls provided with Outlook calendars only allows for items that you do not wish to be displayed to other users through a shared Outlook calendar being marked as "Private" (using Microsoft Outlook "options" functionality setting). However, you can not rely on the Private feature to prevent others from accessing the details of the calendar items. Never use public electronic calendars, such as Google, MSN, AOL or Yahoo calendars, for VA business. Public electronic calendars are not VA-approved.

Can employee information be sent using Outlook email?
Yes. If it is the employee's name only, then this is acceptable. If other information is included that would be considered individually identifiable, it must be encrypted.

Can we share PHI in Microsoft Office Lync?
VA employees may utilize MS Lync in the performance of their job duties knowing that there is a guaranteed end-to-end encryption, including the transfer of sensitive information (PII or PHI) if allowed by their organizational policy. When transferring VA sensitive information in a message, make sure automatic saving of messages in your Outlook conversation history folder is off (default setting), as these files are not encrypted in Microsoft Outlook.

Lyncshould not be used for communicating patient information that is required to be maintained within CPRS to preserve continuity of care. Lync is not part of a VA system of records. Never use a mobile phone's text messaging feature to send VA sensitive information.

If you put a hyperlink in an email message and the hyperlink leads you to a site that has sensitive information are you required to encrypt the message? No. The message does not need encrypted if the link contains no III/PHI. If the link is accessed, there should be appropriate safeguards to stop unauthorized people from gaining access to the information.

Can VHA use email to communicate a program or benefit to Veteran(s) using email?
Yes. Communications about a new VA program or VA benefit does not fall within the definition of "marketing" if there is no commercial component to the communication and as long as this email does not contain III or PHI. Care must be taken in communicating a benefit that is specific to a health condition, i.e. Cardiology, which may potentially infer that the Veteran has a specific cardiology health concern. There is no guarantee that the email used would only be seen by the Veteran, another individual, or other family members who share the same email account. Thus, this communication needs to be one-way.

If sending non-PII or PHI communication to more than one Veteran, there are various options available. A facility policy on emailing using one-way communication is recommended.

All communications must receive approval as designated within policy. It is recommended this person be the Privacy Officer or designee who can ensure no privacy information and/or marketing information is disclosed.

- Place a disclaimer within the email that this message is not secure and recipients should not reply back to the sender with any protected health information or individually identifiable information. Email should contain a facility contact telephone number. It is recommended this disclaimer be place at the very beginning of the email. Example of a disclaimer:

  *This email is provided for informational purposes only. Please do not reply to this email directly. Do not communicate any individually- identifying information or your protected health information via email as VHA will not reply back due to privacy concerns. Veterans are encouraged to use Secure Messaging that is available through MyHealtheVet. If you have any questions concerning this email, please contact <Insert Name and telephone number>.

  - If the recipient does reply back to the sender and the message contains III or PHI, the sender may not reply back on this email but contact the recipient directly by mail or telephone.

- If you are not using mail merge which allows a separate email to be sent to each recipient, multiple email addresses must be placed in the Bcc (blind carbon copy) of the Outlook email as entry in the “to” or “cc” field within Outlook would be considered a privacy breach.
- The “to” recipient will be a VA email account, usually the same sender of this Veteran group email communication.

NOTE: The use of “NoReply&NoReplyAll” only works within the VA domain (va.gov).

Dissemination: Please share with program offices or facility departments you feel would benefit from this information.

Rescissions:
July 2010, May 2012, May 2014

If you have any questions please contact the VHA Privacy Issues Mail group or visit the VHA Privacy Office Website.

OFFICE OF RESEARCH AND DEVELOPMENT
VETERANS HEALTH ADMINISTRATION

Draft Guidance on the Use of Electronic Mail and Electronic Text Messaging for Recruiting and Communicating with VA Subjects in VA Research

Date: July 28, 2017

Draft Guidance

This draft guidance document is being distributed for comment purposes only.

Document issued on July 28, 2018.

This draft guidance is a new ORD guidance document.

Please submit comments and suggestions regarding this draft document within 120 days of the date of issue. Submit comments and suggestions to the VHA Office of Research and Development at VHACOORDRegulatory@va.gov.

SCOPE: This guidance document provides guidance for VA Investigators and VA research team members on the use of VA electronic mail (email) and text messaging for the purposes of recruitment of VA subjects and communicating with VA subjects in the conduct of VA research. ORD's requirements for the protection of human subjects in VA research and the operation of the Institutional Review Board(s) (IRB) for VA facilities are described in VHA Handbook 1200.05. This ORD guidance is based on the recognition that (a) VA employee emails and VA text messages may be subject to the Freedom of Information Act (FOIA), (b) the privacy and confidentiality of VA subject information sent and received by electronic email or text messaging must always be considered, (c) email and test messaging are not secure and may be seen by others, and (d) the IRB is responsible for ensuring that appropriate safeguards exist to protect the rights and welfare of individuals being recruited for research studies and for research subjects. Email is not inherently confidential and VA researchers should have no expectation of privacy when using government mail systems. The following questions are discussed in this guidance document:

1. Can email messages be sent by VA Investigators to recruit and communicate with VA subjects?
2. Can text messages be used by VA Investigators to recruit and communicate with VA subjects?
3. What are examples of personally identifiable information (PII) that VA Investigators cannot send by emails or by text messaging unless the information is encrypted using a VA-approved encryption method?
4. What are examples of protected health information (PHI) VA Investigators cannot send by emails or by text messaging unless the information is encrypted using a VA-approved encryption method?
5. What should a VA Investigator do if she or he receives PII or PHI from a prospective subject or a VA subject by unencrypted email or text message?

6. What is an example format for a study reminder to a VA subject?
7. What are some considerations for an IRB evaluating a research study proposing to utilize email and/or text messages to recruit or communicate with VA subjects?
8. Can a VA Investigator communicate research study information which includes individually identifiable or personally identifiable information to a study recruiting VA employees using VA email?
9. Are VA Investigators required to keep copies of emails and text messages sent to and from VA subjects?
10. Can VA Investigators utilize My HealtheVet's Secure Messaging system to recruit VA subjects in approved VA research studies?
11. Can VA Investigators utilize MyHealtheVet's Secure Messaging system to communicate with VA subjects in approved VA research studies?

1. Can email messages be sent by VA Investigators to recruit and communicate with VA subjects?

Yes. VA Investigators can use VA email to recruit prospective VA subjects and to communicate with VA subjects who have consented to participate in a VA research study as described in the IRB-approved research study. VA Investigators may not utilize their personal email accounts (e.g., Google) or university email accounts for research communications with prospective or consented VA subjects. The use of personal email account or the use of a personal email system to conduct official agency business is not allowed. No PII/PHI can be sent by a VA Investigator for VA research purposes to a prospective or consented VA subject by email unless the email is encrypted using a VA-approved encryption method. Your local ISO should review the encryption to ensure it meets all applicable requirements. If the message is not encrypted, ORD recommends that the email message be reviewed as part of IRB review process. The IRB should consult with the VA Facility's Privacy Officer concerning privacy issues outside the scope of the human subject protection regulations.

Note: An external recipient of a VA RMS encrypted email requires enrollment in the VA's external RMS system in order to open the email at the present time.

2. Can text messages be used by VA Investigators to recruit and communicate with VA subjects?

Yes. Text messages can be used by VA investigators to recruit prospective subjects and to communicate with VA subjects who have consented to participate in a VA research study as described in the IRB-approved research study. VA Investigators may not utilize their own personal devices, such as personal cellphones, personal Instant Messages (IMs), or university owned devices to send and receive text messages with prospective or consented VA subjects. No PII/PHI or identifiers can be sent by a VA Investigator for VA research purposes to a prospective or consented VA subject using text messaging unless the text messaging system is encrypted using a VA-approved encryption method. As indicated above, the ISO and Privacy Officer should review these as part of the review of the protocol.

3. What are examples of personally identifiable information (PII) that VA Investigators cannot send by emails or by text messaging unless the information is encrypted using a VA-approved encryption method?

Personally identifiable information (PII) is considered to be the same as VA Sensitive Information/Data. PII is any information about an individual that can reasonably be used to identify that individual that is maintained by VA, including but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, telephone number, driver's license number, credit card number, photograph, finger prints, biometric records, etc., including any other personal information which is linked or linkable to an individual. (VA Directive 6502)

For purposes of VA research, data which is considered to be PII cannot be sent electronically unless it is encrypted using a VA-approved encryption method. Examples of PII that CANNOT be sent via email unless encrypted include, but are not limited to, the following:

- Names (employee names are acceptable);
- All geographical subdivisions smaller than a State;
- Social Security Number;
- Names of Relatives, including the mother's maiden name;
- Biometric records;
- Fax numbers;
- Electronic mail addresses;
- Any other unique identifying number, characteristic, or code (note this does not mean the unique code assigned by the investigator to code VA research data);
- Any Protected Health Information

In addition to the above list of identifiers described in the HIPAA Privacy Rule, ORD and VHA policy considers a code derived from an individual's Social Security Number to be PII that should not be sent unless it is encrypted.

Additional information regarding sensitive data is described in other VA and VHA Handbooks, including, but not limited to, VA Handbook 6500 and VHA Handbook 1605.01.

NOTE: Even with encryption PII being sent to a non-VA entity requires legal authority to make the disclosure of VHA data.

4. What are examples of protected health information (PHI) VA Investigators cannot send by emails or by text messaging unless the information is encrypted using a VA-approved encryption method?

The HIPAA Privacy Rule defines protected health information (PHI) as Individually-identifiable health information transmitted or maintained in any form or medium by a covered entity, such as VHA. For VA, PHI is considered a subset of PII and includes any health information, not just identifiers or demographics, maintained by VHA that has not been de-identified in accordance with the HIPAA Privacy Rule.

VA Investigators cannot send any PHI to a prospective subject or to a VA subject participating in a VA study unless the email or text message is encrypted using a VA-approved encryption method. The VA National Rules of Behavior require VA employees who access and use VA information or information systems to use VA-approved encryption to encrypt any email, including attachments to the email, which contains VA sensitive information before sending the email. For example, a VA Investigator cannot send the following recruitment email to a prospective subject with the following message unless the email is encrypted because PHI **(in bold)** is conveyed (in addition to ethical issues and IRB regulatory criteria involved in sending this type of recruitment email):

> *"Dear Sir,*
> *You are being asked to participate in a research study because you have been recently diagnosed with **Stage IV Lung Cancer**. Please contact the research team at "AAA-BBB-CCCC".*

In another example, a VA Investigator cannot send the following communication in unencrypted email or text message because the name of the study include information that indicates the VA subject's medical diagnosis :

> *"Dear Ms. X,*
> *This is a reminder that your next study visit for "**Anxiety** Reducing Strategies for **PTSD** Clients" occurs next Monday at 8:00 a.m. in Room 123. Please contact the research team at "AAA-BBB-CCCC" if you need to reschedule. We look forward to seeing you on Monday. Have a great day."*

VA Investigators must be aware of the content of emails and text messages sent as part of the study procedures in a VA research study. The content of the unencrypted email cannot contain any sensitive information. VA Investigators should always consider how the content of the email or text message might compromise the subject's privacy and confidentiality if the message was inadvertently retrieved by someone other than the intended prospective subject or VA subject participating in a VA study. A VA Investigator should not include in the electronic communication information that would allow the reader to conclude that the individual had a specific diagnosis or condition, such as including a signatory line that states, "Research Team for COPD Study". VA Investigators should also not include links to websites in electronic communications that are publicly accessible and would allow the reader to conclude that the individual has a specific diagnosis or condition if the electronic communication was read by others.

5. What should a VA Investigator do if she or he receives PII or PHI from a prospective subject or a VA subject by unencrypted email or text message?

Sending recruitment messages to a prospective subject or communicating with consented VA subjects using the recipient's personal, university, or commercial email accounts should always convey that no PII should be sent by email or text messaging to the VA research team. If health information or PII/PHI needs to be conveyed to the VA research team, it cannot be sent using unencrypted email or text messaging. ORD recommends that a statement be included on any research email or text message stating the following: "Email [or texting] is not secure. Please do not reply back to this message with any personal information or personal health information. Please call INSERT #.

Even though it is not anticipated, there may be rare circumstances in which a prospective subject or a VA subject participating in a VA study sends PII or PHI as part of a response using the individual's personal email or text messaging. The VA Investigator should either respond by telephone to the individual or respond using email or text messaging with redaction of any PII or PHI conveyed by the prospective subject or VA subject participating in a VA study. In addition, the VA Investigator should not forward the email to other VA employees without encrypting the email or test message.

For example, a prospective subject sends the following email to the VA research team after receiving a recruitment email brochure approved by the IRB of Record for the specific VA study using the email address on the IRB-approved electronic recruitment flyer:

> *"I am so excited to receive information about this research study. I would love to be in it. I just happened to see my physician this morning, and he placed me on Norvasc and Captopril and told me that I have worsening COPD, with an oxygen level of 72 and a carbon dioxide level of 56. Please help me understand what this means. I will also send you my labs when I get them."*

In the above example, no telephone number was provided by the prospective subject. The VA Investigator cannot respond back using unencrypted email if any PII/PHI is going to be included. Therefore, the VA Investigator could send back an email as follows:

> *"Our research team received your email indicating interest in the study. You also had questions about your health. Please give me a call at INSERT # at your convenience."*

6. What is an example format for a study reminder to a VA subject?

Study reminders sent by a VA research team by email or text messages cannot contain any PII or PHI unless the communication is encrypted using a VA-approved encryption method. Study reminders can be sent by a VA research team without including information that would require encryption. The content should not include any information that would indicate the type of appointment or the specific location, or specific diagnosis or condition; the content must be reviewed by the IRB as part of the IRB approval of the VA research study.

For example, the following is a study reminder that could be sent without encryption because no sensitive data is included in the content:

> *"Reminder: You have a visit on May 4, 2016 at 8:30 a.m. Please call 111-222-3333 if you need to reschedule or have questions."*

This is an example of a study reminder which contains PII/PHI and <u>cannot be sent</u> without encryption:

> *"**C70298** Study Reminder: You have an appointment with the **C70298** Study team on **May 11, 2016 at 8:30 a.m**. in Room 115 on the 1st floor of the main hospital building. Please bring all unused study medication and your*

*supplemental **Albuterol inhalers** to the study visit. Please call the **Pulmonary Clinic** at 111-222-3333 if you need to reschedule or have questions."*

7. What are some considerations for an IRB evaluating a research study proposing to utilize email and/or text messages to recruit or communicate with VA subjects?

The use of VA email in a VA research study must be evaluated by the IRB. When research studies utilize email or text messaging, the IRB must review the content of standardized communications. Other considerations for the email or text messages include, but are not limited to, the following:

- The VA Investigator must employ measures to avoid disclosing the email addresses of potential research subjects or other consented subjects to others. Common techniques include the use of:
  (a) Individually targeted messages (only one address in the "TO" line per message)
  (b) Group targeted messages with all recipient email addresses in the "BCC" line". NOTE: Sending a group message with all recipient email addresses in the "TO" or "CC" line is inappropriate as all recipients can see the email addresses of the group.

- The VA Investigator should use a standard "SUBJECT" line that does not indicate the name of the study or the name of the recipient or other individually unique identifier. For example, the "SUBJECT" line should contain wording that would be general in nature and not indicate that the individual is being recruited for a study. This will prevent others who may see the list of emails received but cannot open them from knowing that the individual is being recruited. For example, the "SUBJECT" line should <u>not</u> read, "VA Subjects needed for Study on Addiction in Health Care Providers". SUBJECT lines cannot be encrypted.

- There should be a signature block for the person sending the email, including his or her contact information at the VA but the contact information cannot contain anything that would indicate the specific study. The VA Investigator's non-VA contact information should not be included for a VA study. There should also be a name and VA contact information for a VA research staff member who would be able to answer questions related to the study (if different than the VA Investigator). No responses related to the study which includes PII/PHI can be sent using unencrypted VA email or text messaging by a VA Investigator or VA research team.

In order to approach human subjects research requiring IRB approval, the IRB is required to determine that all of the IRB approval criteria are met, which includes equitable selection of subjects and if there are adequate provisions to protect the privacy of subjects and to maintain the confidentiality of data (38 CFR Part 16.111(a)(3) and (a)(7)). The IRB should consider how the contact information, such as email addresses for sending IRB-approved recruitment information, is being obtained by the VA Investigator for the study. Similar to IRB considerations for contacting prospective subjects by telephone for recruitment activities or obtaining follow-up information for VA subjects in a VA study or sending letters by mail, the IRB should also consider how many emails or text messages are sent to prospective subjects for recruitment purposes

or to VA subjects participating in a research study. The IRB should evaluate whether the frequency and/or content is appropriate for the purpose of the research study or evaluate whether or not the frequency and/or content could be considered to be coercive or harassment by prospective subjects or VA subjects participating in a research study.

The IRB cannot approve an informed consent process which uses email or text messaging to document informed consent as described in VHA Handbook 1200.05. ORD permits informed consent for VA research to be obtained electronically, but the informed consent process and documentation must meet all requirements described in VHA Handbook 1200.05 as well as applicable VA requirements. Documentation of informed consent by email or text messages is not an example of consent which is obtained electronically permitted under VHA Handbook 1200.05, Paragraph 16(e)(2)(c). In addition, neither of these types of electronic communication can serve as a signed HIPAA authorization for use and disclosure of PHI for research purposes.

8. Can a VA Investigator communicate research study information which includes i personally identifiable information to a study recruiting VA employees using VA email?

VHA conducts numerous studies involving VA employees, and encrypted email using a VA approved encryption method can be used to communicate sensitive information, such as personally identifiable information, between a VA employee and a VA research team if approved by the IRB as part of its approval of the research study. However, it is important to remember that the privacy and confidentiality of VA employees who are asked to participate in VA research must be evaluated by the IRB when using email or text messaging, regardless of whether PII is being sent using encrypted VA email or unencrypted email is being sent by a VA research team member to VA employees.

The content of the message should not include any information that might compromise the employee's privacy, position, or standing as a VA employee if others, such as the employee's supervisor, were to know that he or she was being approached to participate in the project or has consented to be in a VA research study. VA employee email is not confidential and is subject to review by VA. Some VA employees routinely give permission to others (e.g., administrative assistants) to allow them to read the individual's emails. VA also may be required to release VA employee emails under a FOIA request.

The IRB should consider whether or not additional privacy and confidentiality safeguards are needed when VA employees are recruited as VA subjects, regardless of whether or not email or text messaging is involved for the VA research study.

9. Are VA Investigators required to keep copies of emails and text messages sent to and from VA subjects?

Emails and text messages sent and received by a VA Investigator and the VA research team are federal records subject to the VHA Record Control Schedule. Copies of the email communications and text messages sent and received by a VA Investigator and the VA research team must be maintained in accordance with the VHA Record Control Schedule (RCS 10-1) as part of local VA Investigator records.

Text messages may have unique issues for retention because they are not retrievable in the same context as email messages. However, the text messages sent and received in VA research must be printed or captured as part of VA's record retention requirements. If they cannot be retained, then these forms of communication cannot be used.

10. Can VA Investigators utilize My HealtheVet's Secure Messaging system to recruit VA subjects in approved VA research studies?

VA Investigators cannot use My Health***e***Vet's Secure Messaging system to recruit VA subjects.

11. Can VA investigators utilize My HealtheVet's Secure Messaging system to communicate with VA subjects in approved VA research studies?

At this time, VA investigators cannot send and receive research-related communications as part of a VA-approved research study, however this capability is currently being explored. Additional guidance will be provided

REFERENCES:

VA Handbook 6500 (May 10, 2015): Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program

VA Directive 6301 (April 24, 1997): Electronic Mail Records

VA Directive 6502 (May 5, 2008) : VA Enterprise Privacy Program

VHA Handbook 1200.05 (November 12, 2014): Requirements for the Protection of Human Subjects in Research

VHA Directive 1605.1 (August 31, 2016): Privacy and Release of Information

VHA Privacy Fact Sheet, Volume 10, No. 5 (May 2014): Use of Individually identifiable Information in Microsoft Office Applications and VistA