Office of Informatics and Analytics
VHA Privacy Office

Privacy Fact Sheet

May 2014 ***Volume 10, No. 5***

Use of Individually Identifiable Information in Microsoft Office Applications and VistA

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, Text Messaging and VistA E-Mail. 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 Handbook 1605.1 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 Handbook 1605.1, Appendix on de-identified information 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 http://vaww1.va.gov/MYHEALTHEVET/Secure_Messaging.asp

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). It is OK to send a text message as you would leave a voice mail message for a Veteran. You cannot mention specific locations of appointments and any additional information except as follows:

Reminder: You have an appointment on January 29, 2013 at 3:00 pm. Please call 321-123-3213 if you have any questions.

Can a provider get an authorization from a Veteran to allow VA to send III and PHI through email or text message?
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).

NOTE: Text messaging is not a secure form of communication for PII or PHI.

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.

Is it acceptable to use the auto-forwarding option in VistA Mailman to forward emails to Outlook if there is PHI or PII in them?
No. You cannot use the auto-forwarding option in VistA to forward emails that contain III or PHI as they are not encrypted.

Can VistA Mailman messages be autoforwarded to home email accounts?
No. VA Handbook 6500 prohibits auto-forwarding information from VistA that may contain III/PHI to any outside email address as there is currently no capability for encrypting the information.

Can we share PHI in Microsoft Office Lync (Formerly Communicator/Instant Messaging)?
VA employees may utilize MS Lync/Communicator 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.

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

Is it acceptable to send individually identifiable information in the body of a VistA email?
Yes. Full name and full SSN can be used in the body of a VistA Mailman message when needed for unique identification of a patient for purposes of providing treatment or for patient safety issues including notification of erroneous notes. Treatment purposes include the coordination of care between providers or within the multidisciplinary team, consultations, patient alerts, discharge planning, transferring the patient to another care team, etc. The last name, last four numbers of the SSN, date of birth, other account numbers (e.g., bill number), and/or other identifying information may be used in the body of a VistA Mailman message for unique identification of a patient for payment and health care operation purposes.

What is acceptable to place in the subject line of a VistA email message? First initial of last name and the last four numbers of the SSN may be used in the Subject Line of a VistA Mailman message to identify the patient and track the message.

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).

Using Email Merge Function in MS Word.

Rescissions:
July 2010
May 2012 (R)

Privacy Office at a glance…

VHA personnel should contact the VHA Privacy Office via email through the VHA Privacy Issues mail group.

Website: http://vaww.vhaco.va.gov/privacy