Privacy Fact Sheet

August 2020

Use of Protected Health Information in Microsoft Office Applications - Updated

This fact sheet provides guidance to the field on when it is appropriate to include protected health information (PHI) when using Microsoft Office Outlook Calendar, Microsoft Outlook Email, r Microsoft Teams. The guidance is provided in conjunction with VHA Health Care Security Requirements (HCSR) office.

Once privacy and security requirements are met it becomes a VHA Program Office decisions on whether to use a Microsoft (MS) Office application to perform certain program functions. Each VHACO program office is responsible for determining how MS Office applications are used within their purview after privacy and security requirements are addressed. The VHA Privacy Office will refer all questions relating to the use of MS Office applications to the applicable program office when the below applies.

Email

A Veteran cannot give permission for VA to ignore a security policy or requirement. VA Handbook 6500 states that VA sensitive personal information (PII/PHI) cannot be sent via email unless secured (e.g. encryption). However, if the email is secured appropriately through encryption, such as with Azure RMS, all security requirements are met, and if the email is sent to a recipient who has legal authority to receive the PII/PHI, such as a Veteran receiving his own records, the privacy requirements are met. Therefore, the VHA Program Office can make the determination to allow RMS so that the email can be encrypted. This includes allowing communicating with Veterans via email. Along the same lines a VHA Program Office may prohibit such communications based on the policies and needs of its program even when privacy and security requirements are met.

When a VHA Program Office opines on communication tools to be used in a manner that complies with the privacy (i.e., disclosure authority) and security requirements (i.e., encryption) then that is the guidance that will be followed even when the guidance is to prevent use of a specific communication tool. For example, MyHealtheVet requiring Veterans to communicate with their providers using Secure messaging.

Of note, Subject lines of emails are not encrypted and may not contain any PII/PHI per security requirements and may not contain any names (full or partial) or full social security number (SSN) per privacy requirements regarding Privacy Act systems of records. The first initial of the last name and last four SSN by itself is not considered a unique identifier and therefore can be included in the subject line of an email message.

For more information on Azure RMS please reference the following FAQ's and Bulletins at: https://vaww.portal2.va.gov/sites/AIP/_layouts/15/start.aspx#/

Outlook Calendars

MS Outlook calendar controls were not designed to secure sensitive information (PII/PHI). The security controls provided with MS Outlook calendars only allow items that you do not wish to be displayed to other users through a shared MS Outlook calendar to be marked as "Private" (using MS Outlook "options" functionality setting). However, you cannot rely on the Private feature to prevent others from accessing the details of the calendar items. Therefore, Veteran PII/PHI should not be placed in or attached to MS Outlook Calendar invites as there is not a way to encrypt. NOTE: If PHI is needed for a calendar appointment it is best to send the PHI as an attachment in a separate email using encryption.

Never use public electronic calendars, such as Google, MSN, AOL or Yahoo calendars, for VA business. Public electronic calendars are not VA-approved.

Microsoft Office (MS) Teams

VA employees may utilize MS Teams in the performance of their official VA job duties knowing that there is a guaranteed end-to-end encryption, including the sharing of sensitive information (PII/PHI), if allowed by their organizational policy. When a VAMC or VHA Program Office opines on the use of MS Teams in a manner that complies with the privacy (i.e., access authority) and security requirements (i.e., encryption), then that is the guidance that will be followed for that activity. Use of MS Teams for patient-provider communications require approval by appropriate VHA Program Offices.

Data displayed or recorded as part of a MS Teams meeting are not part of a Privacy Act system of records (SOR) though they are an official agency record. Therefore, if used for communicating patient information that is required to be maintained within CPRS to preserve continuity of care, VHACO HIMS and Patient Care Services need to approve. When manually transferring PII/PHI from r a MS Teams message by copy/paste to an email in MS Outlook, ensure the email is encrypted. Only discuss or display PII/PHI via MS Teams with VA employees, contractors or other individuals who have authority to view or receive the PII/PHI.

Important note about MS Teams:

All MS Teams group chats, individual chats, and video meetings are saved to VA servers and will become official agency records covered by official record retention requirements. If users delete chat conversations or videos from MS Teams from their accounts on their computers, that data is still maintained by VA within Microsoft Office 365, and this data is subject to discovery. MS Teams meeting are not automatically recorded. Recording must be initiated and there will be a notification that the meeting is being recorded.

Be aware when communicating in chat you may think that you are communicating with one person when in fact there are additional participants, so be cognizant of the chat session, Teams, Channel or meeting when responding. And do not say anything in a chat that you

would not want made available to the person you are speaking about or made available under eDiscovery.

Remember that chat conversations resume between parties with the conversation starting at the end of the previous chain regardless of how much time as elapsed. This is true for a group chat, such as one associated with an ongoing scheduled meeting, EVEN if the topic has changed and new members have been added. Any new members to a group chat or ongoing scheduled MS Teams meeting can view all previous coversations, meeting chats and recordings. Be careful when adding new attendees to an ongoing scheduled MS Teams meeting to ensure the individuals need access to all of the previous meeting chats and recordings in the performance of their official duties.

It is important that you apply the same level of discretion to MS Teams content as you do to any other communication (e.g., verbal, email, correspondence) per VA's Rules of Behavior.

For more information on MS Teams please reference the following FAQ's and Bulletins at https://dvagov.sharepoint.com/sites/OITEPMOEPMDES/Projects/MSTeams/SitePages/Home.aspx

For questions around the functionality of MS Teams, please reach out to the VA MS Teams PM Team via email at VAMSTeamsPMTeam@va.gov.

Dissemination: Please share with program offices and/or facility services for awareness.

Rescissions:
July 2010, May 2012, May 2014, May 2017, July 2020

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