Use of Encrypted Email with Community Providers: External Rights Management Services

VHA Homeless Programs

This document is intended to provide information on the use of Rights Management Services (RMS) for the encryption of emails containing PII/PHI between VA and external community providers using Microsoft Outlook.

This guide is broken down into the following sections:

- Rights Management Services Overview,
- Instructions for Homeless Program Staff,
- Instructions for Community Providers, and
- Frequently Asked Questions (FAQs).

National Privacy Guidance

Authority to Make Disclosures to Community Partners FAQs

National RMS Guidance

RIGHTS MANAGEMENT SERVICES OVERVIEW

Rights Management Services (RMS) allows VHA Homeless Program staff to securely email sensitive information to approved external community providers. RMS encryption works with Microsoft Outlook and GigaTrust to enable community providers to view and reply to emails containing encrypted protected health information (PHI) sent by VHA Homeless Program staff. To be eligible to use RMS, the community provider must have all of the following: 1) Administrative rights to install the GigaTrust application on the computer, 2) Microsoft Outlook 2007 or higher; and 3) Windows 7 or higher. Community providers without administrative rights to their computers will require assistance from their local Information Technology (IT) Department in order to use RMS. Users may also require the assistance of IT if there is a firewall or anti-virus software in place.

Other technical assistance resources related to privacy and information sharing are available on the Homeless Programs Operational Planning Hub at the following link: http://vhaindwebsim.v11.med.va.gov/hub2/hp/.

You can also send an email to the Homeless Programs RMS Support Team if you have questions about the information contained within this document.

TABLE OF CONTENTS

Hold the <control> button and click on the hyperlink to go directly to the scenario form for specific details.

INSTRUCTIONS FOR HOMELESS PROGRAM STAFF

Registering a New User

To begin using RMS with a trusted community partner, VHA Homeless Program staff must first register the user for an external RMS account. On the External RMS Request SharePoint Site, scroll to the bottom of the webpage and click "add new item." The external user's email address, first name, last name and a justification statement is needed identify why the community provider needs access to encrypted information via email. The requesting staff will also need to enter his or her supervisor's information in the "Requester's manager" field prior to submitting the request. Click on the address book icon to the far right of the text field in order to browse the directory and select the appropriate supervisor. A verification email will be sent to the requestor's email address once the request has been processed.

Sending an Encrypted Email

Once the request has been processed and approved, the requestor will receive an email confirmation. After verifying that the community provider has completed all the steps outlined in the "Instructions for Community Providers" section below, a secure email may be sent to the approved email address. In Microsoft Outlook, click on the "Home" tab and select "New E-mail." In the new message window, click the "Options" tab, select the "Permission" button dropdown, and then select "Encrypt Only" or "Do Not Forward." Text will then display at the top of the message indicating that "Encrypt Only" or "Do Not Forward" permissions have successfully been applied to the message. Proceed with typing and sending the secure message.

Sending Encrypted Attachments in an Email

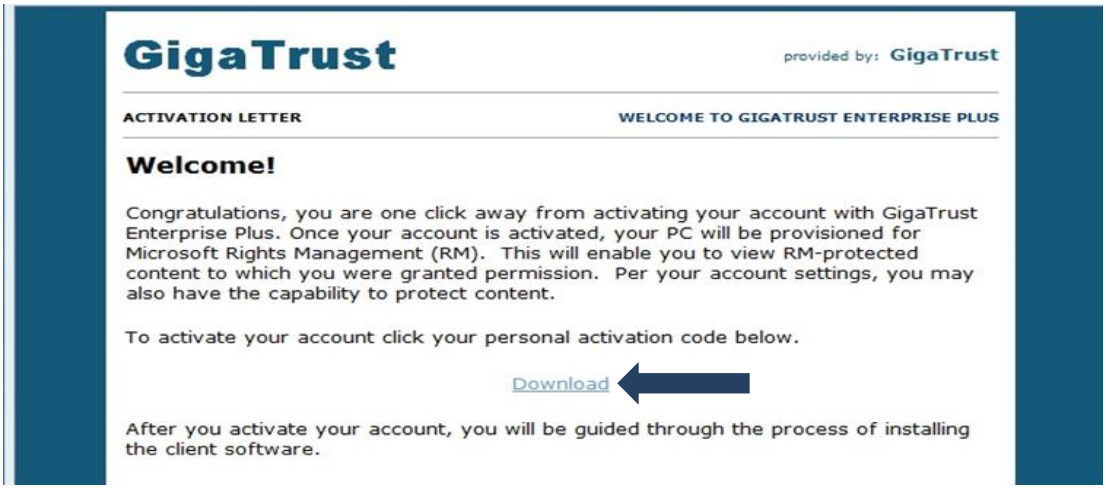
When attaching a file to the email, an alert will appear that states, "Only file attachments that support rights management will automatically have their permission restricted to match the restrictions on this e-mail. All other file types are attached unprotected." Note that only Microsoft products, such as Word and Excel, may be sent securely through RMS. Other file types, such as Adobe PDF, may not be encrypted for secure emailing outside VA. A list of accepted file types can be accessed here.

INSTRUCTIONS FOR COMMUNITY PROVIDERS

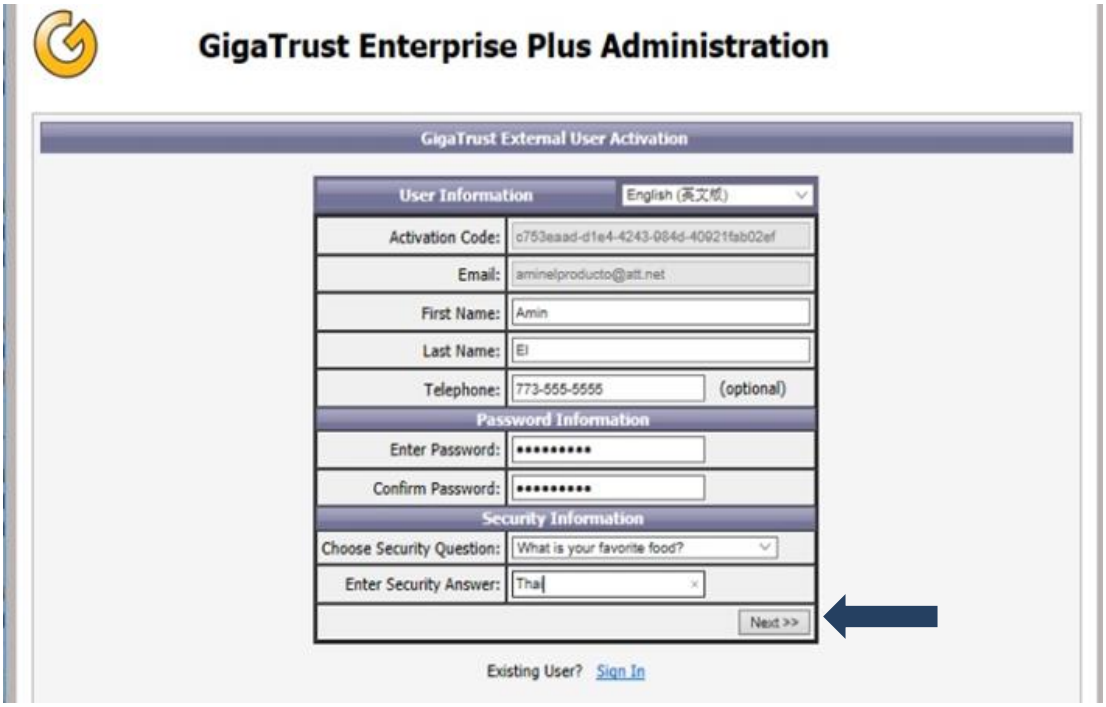
Note: The directions provided below are intended to serve as a general guide. Displays may vary based on the Windows or Outlook version, permissions, and settings.

Installing GigaTrust

1) Once the community provider has been approved to begin using RMS, the following email will be sent to the approved email account. Before beginning the installation process, check to make sure that the popup blocker is disabled in the internet browser. Please also note that anti-virus software may prevent the download and installation of GigaTrust. If applicable, be sure to check these settings. Click on "Download."

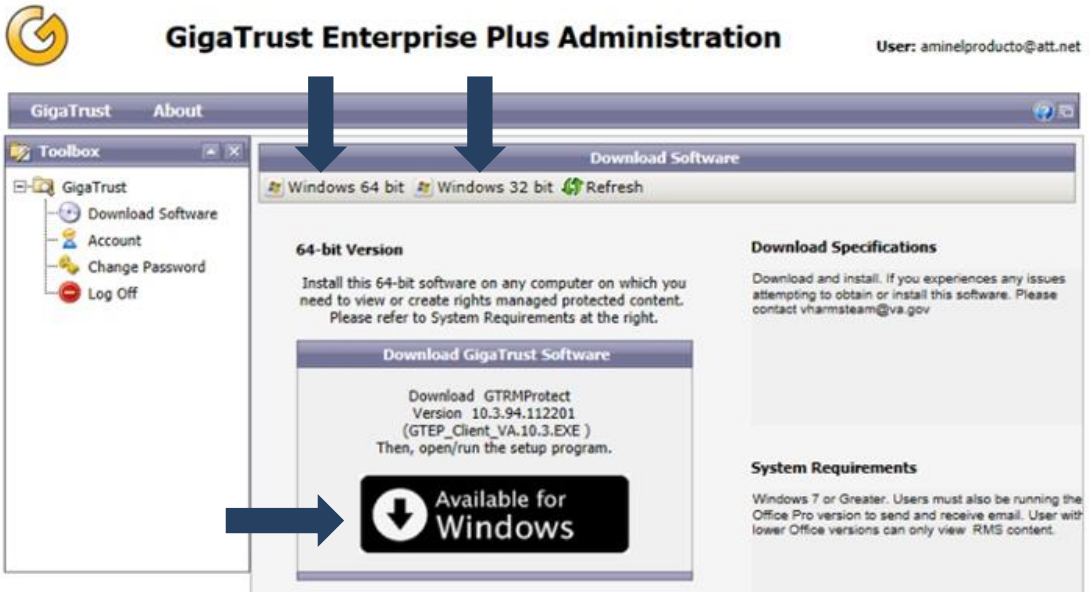


2) Enter the required information and click on "Next."

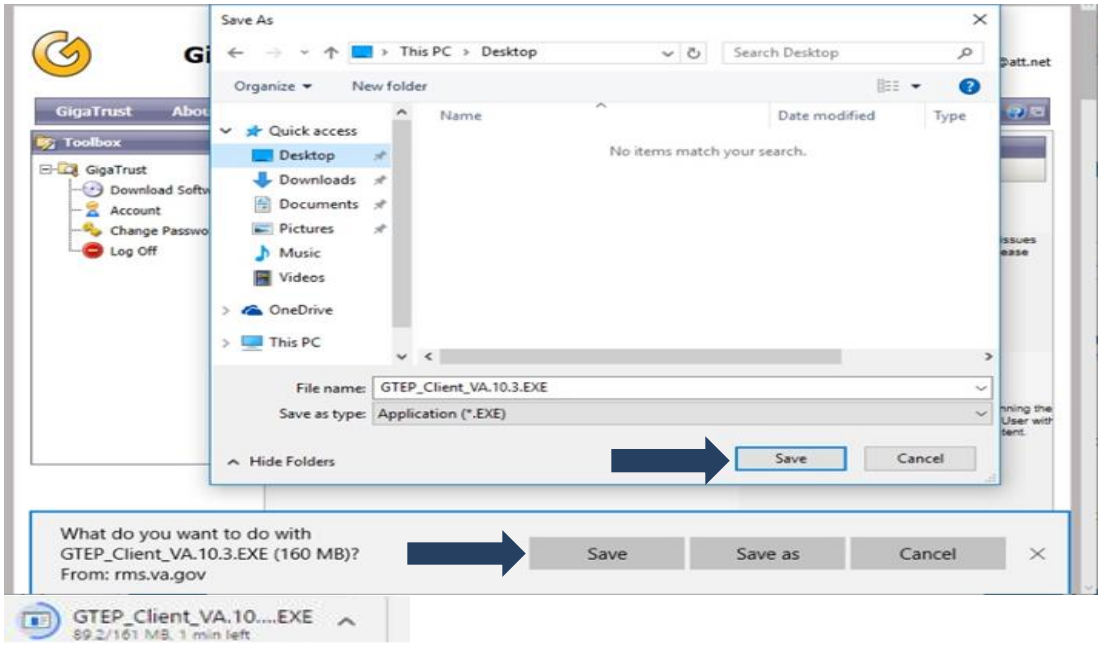


3) Select the appropriate install version (32-bit or 64-bit). To determine which version to download, open Microsoft Outlook and click on the "File" and then click "Help." Under "About Microsoft Outlook," either (32-bit) or (64-bit) will display in the "Version" field. After making the appropriate selection, click on the "Available for Windows" button followed by "Download Now."

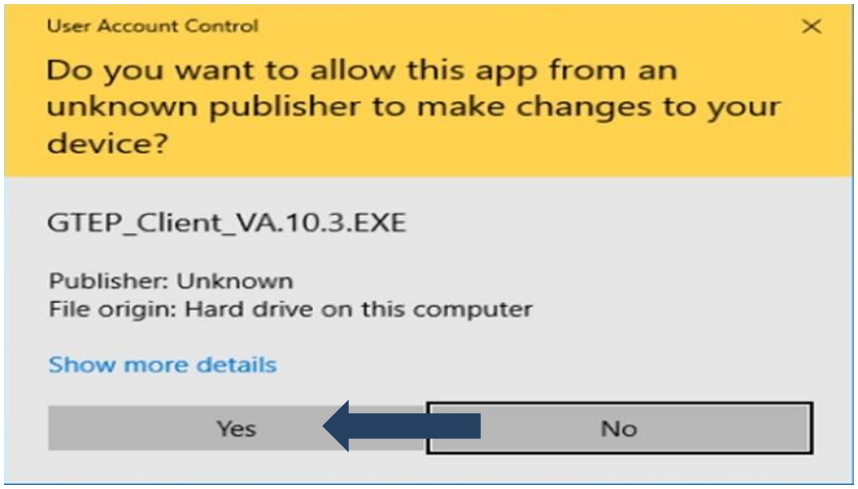
Note: Microsoft Office should be closed before beginning the installation process.



4) If the download does not begin automatically, a pop-up bar will generate at the bottom of the screen. Click "Save."

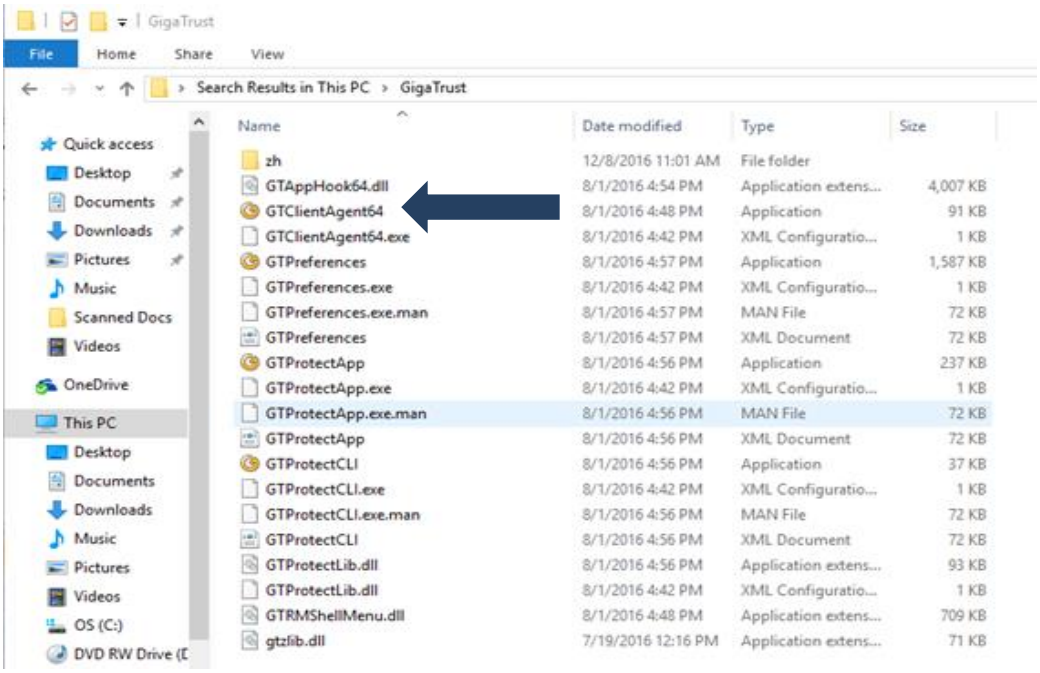


5) If the User Account Control dialogue box does not populate automatically, click on the completed download, as displayed in step 4 above, in order to proceed with this step, and then select “Yes.”

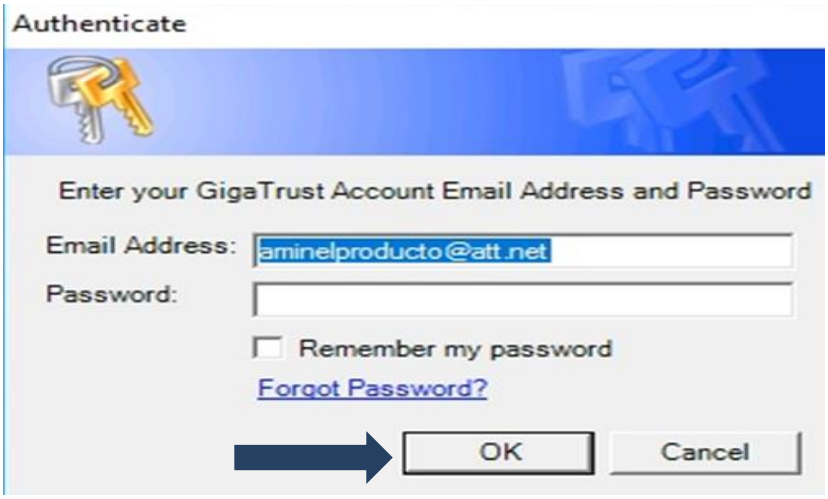


6) GigaTrust client will proceed to install. Please reboot the machine after this process has completed.

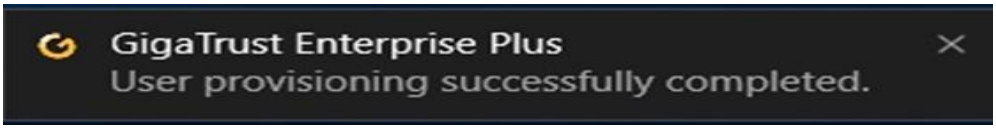
7) Once the machine has restarted, verify that the application has been correctly installed by searching the PC for “GigaTrust.” Once located, double click “GTClientAgent64” to begin using the application.



8) Enter the email and password associated with the GigaTrust account (Step 2), and click "OK."



10) The following pop-up will display, indicating that installation was successful.

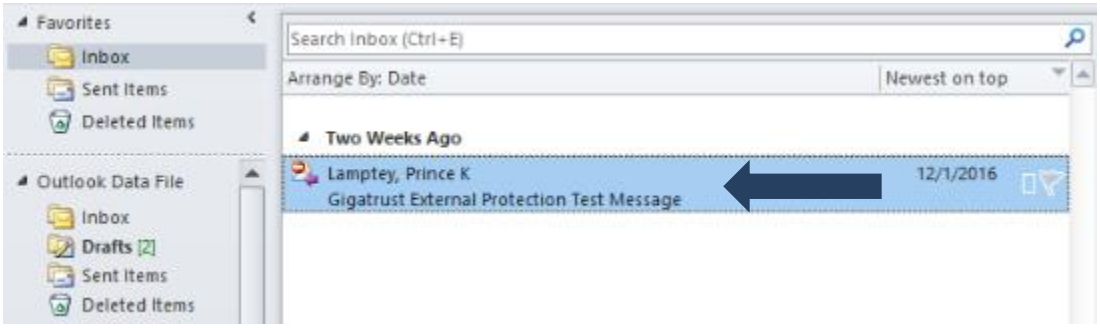


Opening an Encrypted Email

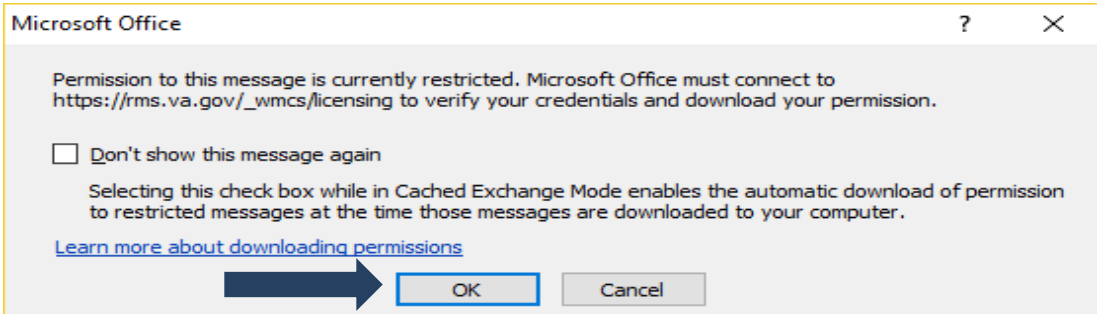
Note: Steps 1-5 of this section must be completed successfully before proceeding with the use of RMS for sharing PHI.

1) After launching Microsoft Outlook, an encrypted email with the subject "GigaTrust External Protection Test Message" should be located in the Inbox. If this email is not able to be located in the Inbox, please check the Junk E-Mail folder.

2) Double click to open the test message.



3) A Microsoft Outlook alert will populate to confirm the connection with RMS in order to download restricted message. If you do not want to receive this alert in the future, click the check box "Don't show this message again," then click "OK."



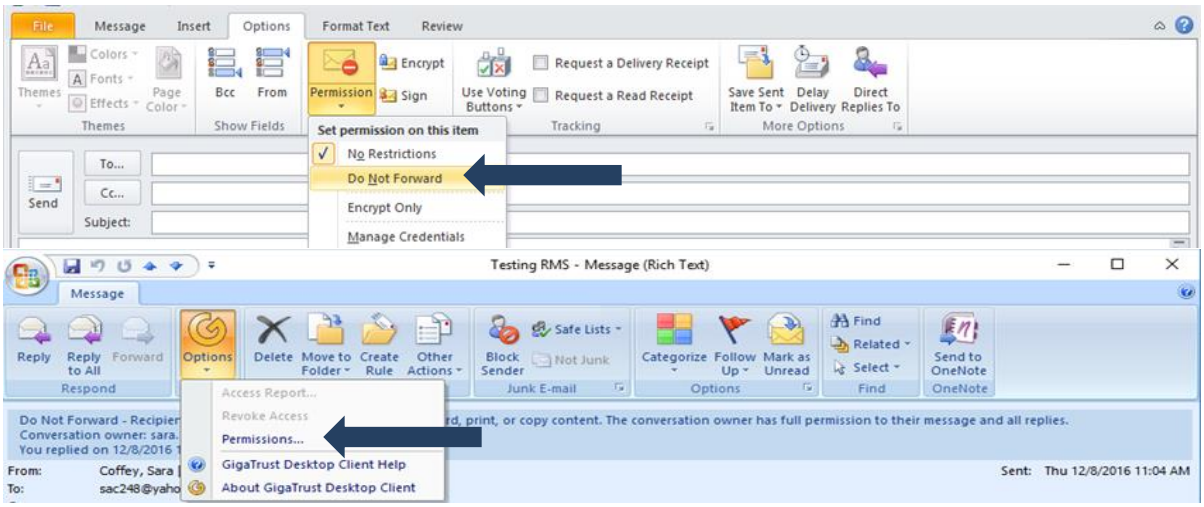
4) The encrypted email should then open in Outlook. Note that it make take several moments to establish the connection with RMS in order for the message to populate. If you receive an email with an attachment labeled "message.rpmsg," please send a message to the Homeless Programs RMS Support Team email group informing that you have received this attachment in error and require further support.

5) If the test message opened successfully, please proceed with using this process to view encrypted emails from VHA Homless Program staff.

Replying to an Encrypted Email

1) When responding to an email from a VHA Homeless Program staff, click on "Reply" or "Reply All" at the top of the original email. Encryption should be retained from the original email, indicated by an encryption statement or "Do Not Forward" message ribbon at the top of the email.

2) To verify encryption settings or to send an encrypted response to an unencrypted email, navigate to the "Permission" section of the message and ensure that "Do Not Forward" is selected. The location of the "Permission" section may vary, as shown below. Note that Outlook accounts outside VA will not display an "Encrypt Only" option. Selecting "Do Not Forward" not only encrypts the message, but also ensures that the recipient cannot forward the contents to another user that has not been approved to use RMS.

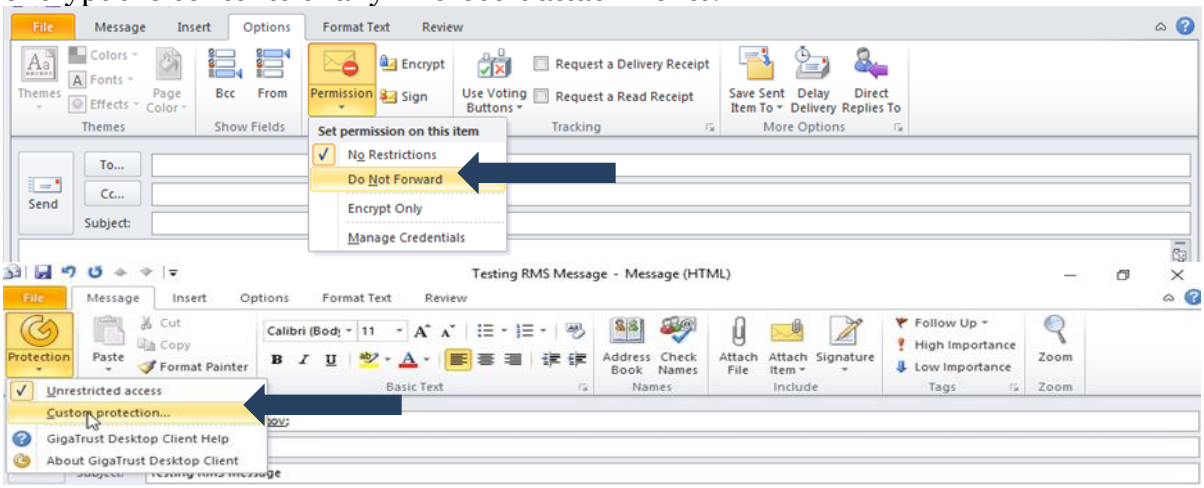


3) Once the "Do Not Forward" ribbon appears, proceed with composing and sending the email.

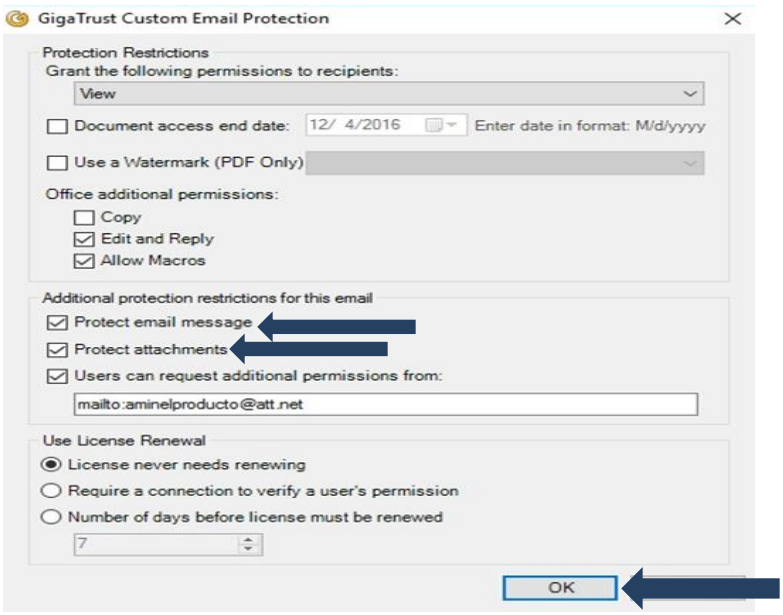
Composing a New Email

1) In a new Outlook message, begin by entering the recipient's information into the "To" line to designate who should have permission to view the contents of the message.

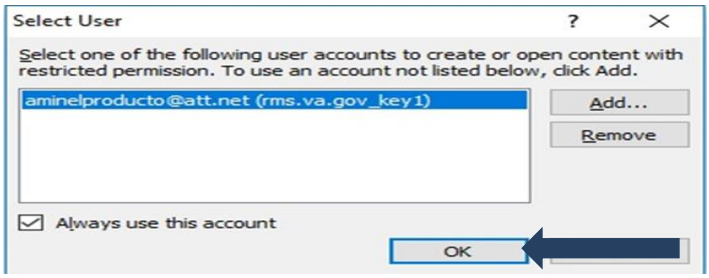
2) Depending on the version of Outlook used, select the GigaTrust Protection dropdown and click "Custom Protection." If the GigaTrust icon is not available, select "Do Not Forward" and proceed with typing and sending the email. Note that "Do Not Forward" will automatically encrypt the contents of any Microsoft attachments.



3) If using the GigaTrust Custom Email Protection option , select the custom parameters specific to the permissions needed for the email, then click "OK." If the message contains attachments, be sure to select both "Protect email message" and "Protect Attachments." Note that this feature is not available for older versions of Outlook, though encryption is still in place for messages and their attachments.



4) Verify the recipient's email address, and click "OK" to send the message.



5) The following message will display, verifying that the contents of the email have been encrypted using GigaTrust.

RIGHTS MANAGEMENT SERVICES FAQS

Who should use RMS?

RMS is appropriate for use between VA and approved external email accounts. However, it is important to note that RMS may not work correctly for all community providers due to various compatibility issues described in the overview and instructional portions of this guide. Due to these issues and steps involved in gaining RMS access, it is recommended that homeless programs identify a single point of contact for each community agency requiring access to encrypted emails from VHA Homeless Program staff. This will help to expedite the approval process for RMS users across homeless programs.

How long will it take for a community provider to be approved to use RMS?

The VHA RMS Team works to approve requests as quickly as possible. This involves a review of the VHA Homeless Program staff's request for access and entering specific approval for each new user's external email account. Process timeframes depend on the number of requests pending approval at a given time. However, average process time is approximately two to three business days. The community provider will receive an email notification when approval has been granted.

When should I encrypt emails to community providers?

As with emailing PHI within the VA email system, emails to community providers outside the VA email system should be encrypted with RMS any time the contents include sensitive, Veteran identifying information. Examples include corresponding with a Public Housing Authority (PHA) about the status of a Veteran's voucher or sharing By-Name List (BNL) information with a community partner.

What information can I share with community providers using RMS?

The same rules would apply for communication using RMS as with any other form of communication. Please refer to the National Privacy Guidance and the Authority to Make Disclosures to Community Partners FAQs for additional information.

What should the community provider do if they receive error messages or Windows Security alerts when attempting to use RMS?

Since RMS uses both Outlook and the GigaTrust application, errors and other alerts are typically the result of a glitch establishing the connection between these systems. In this case, this is resolved by restarting the computer. If the issue persists, community providers should work with their local IT department to ensure that permissions and firewall settings will permit use of GigaTrust.

What should the community provider do if encrypted emails can be shared successfully but attachments are not able to be sent or opened correctly?

This is usually the result of the firewall stripping attachments from the encrypted email. Resolving this will typically require assistance from the community provider's local IT department to adjust the agency's firewall settings and add specific exemptions for RMS.

Whom should I contact if I have questions about RMS?

Questions or issues regarding RMS may be sent to the Homeless Programs RMS Support Team email group.