Administration for Community Living Office of Healthcare Information and Counseling

Managing Through COVID-19 Work grouP - September 2020

Delivering Protected Identifiable Information (PII) Guidance Options

Preparing for Remote Medicare Open Enrollment Toolkit

A close up of a logo

Description automatically generated

Contents

[Overview 1](#_Toc49466176)

[Why privacy & confidentiality is important 1](#_Toc49466177)

[Determining confidentiality 2](#_Toc49466178)

[Related ACL Volunteer Risk and Program Management (VRPM) policies for SMPs and SHIPs 3](#_Toc49466179)

[Using Print to Mail or fax to send confidential information 3](#_Toc49466180)

[Using Microsoft Outlook to send confidential emails 4](#_Toc49466181)

[Using gmail to send confidential emails 8](#_Toc49466182)

[Creating a Microsoft Word password-protected document 11](#_Toc49466183)

[Creating an Adobe Acrobat password-protected document 14](#_Toc49466184)

[Using fillable online forms to collect confidential information 19](#_Toc49466185)

[Beneficiaries and receiving PPI guidance 21](#_Toc49466186)

# Overview

This resource is intended for ACL grantee internal use. When working with counselors and beneficiaries this document will ensure you have outlined guidance to send to the beneficiary on “sending” and “receiving” information related to PII electronically. Choosing which platform works for your organization and/or the beneficiary is important. Remember to look at your organization’s current policies and procedures when making these choices to ensure you have the information and resources needed. Finally, keep in mind a few red flags:

* Encrypted types of documents and/or emails can appear within junk mail folders. Remember to check there for items.
* Be aware of file sizes. Receivers can have file size restrictions.

# Why Privacy & Confidentiality is Important

1. It allows clients to share personal information that ACL grantees need to do their work.
2. It shows respect for clients and helps to protect them.
3. It builds your program’s reputation as a trusted, reliable resource.
4. It helps to prevent costly privacy and potential security breaches.

# Determining Confidentiality

It is important to determine whether the information you are sending is confidential. Individual identifiable health information is information that should be sent as protected information. The options in this resource provide different ways of sending this confidential information electronically.

“Individually identifiable health information” is information, including demographic data, that:

* relates to an individual’s past, present or future physical or mental health or condition,
* relates to providing health care to the individual, or the past, present, or future payment for providing health care to an individual, and,
* identifies the individual or gives a reasonable basis to use in identifying an individual.

Individually identifiable health information includes common identifiers like, name, address, birth date, Social Security Number.

This information may include common identifiers such as:

* A client’s name
* Address
* Birth date
* Medicare number
* Social Security number

Information going out to beneficiaries or other team members from an ACL grantee that would not need to be protected would include:

* Plan comparisons
* Plan enrollment confirmation
* Brochures on the program, fraud prevention, or identity theft

# Related ACL Volunteer Risk and Program Management (VRPM) Policies for SMPs and SHIPs

4.2 Internet protocol [Required]

*Policy:* The SMP/SHIP has a protocol for use of the Internet, covering email use and appropriate access to web sites.

The SMP/SHIP has in place a protocol and appropriate training for volunteers who use wireless devices to connect to the Internet while performing SMP/SHIP work.

The SMP/SHIP has a protocol and appropriate training for volunteers who make use of their personal computers while performing SMP/SHIP work.

**3.94 Confidentiality [Required]**

*Policy:* Volunteers are responsible for maintaining the confidentiality of all proprietary or privileged information to which they are exposed while serving as a volunteer, whether this information involves a member of staff, a volunteer, a beneficiary or other person, or involves the overall business of the SMP/SHIP.

Volunteers take all steps necessary to safeguard the confidentiality of all SMP/SHIP and beneficiary related information and to prevent personal information of beneficiaries from falling into the possession unauthorized persons.

Volunteers use any information collected or obtained in their course of their SMP/SHIP work only to assist the beneficiary or otherwise fulfill volunteer role responsibilities. No information collected or obtained in the course of SMP/SHIP work is disclosed other than when clearly approved by an authorized SMP/SHIP representative.

There is zero tolerance for breaches of confidentiality in connection with work at the SMP/SHIP.

# Using “Print to Mail” or Fax to Send Confidential Information

When a secure electronic transfer option is not available, the best option is to print the document out and then:

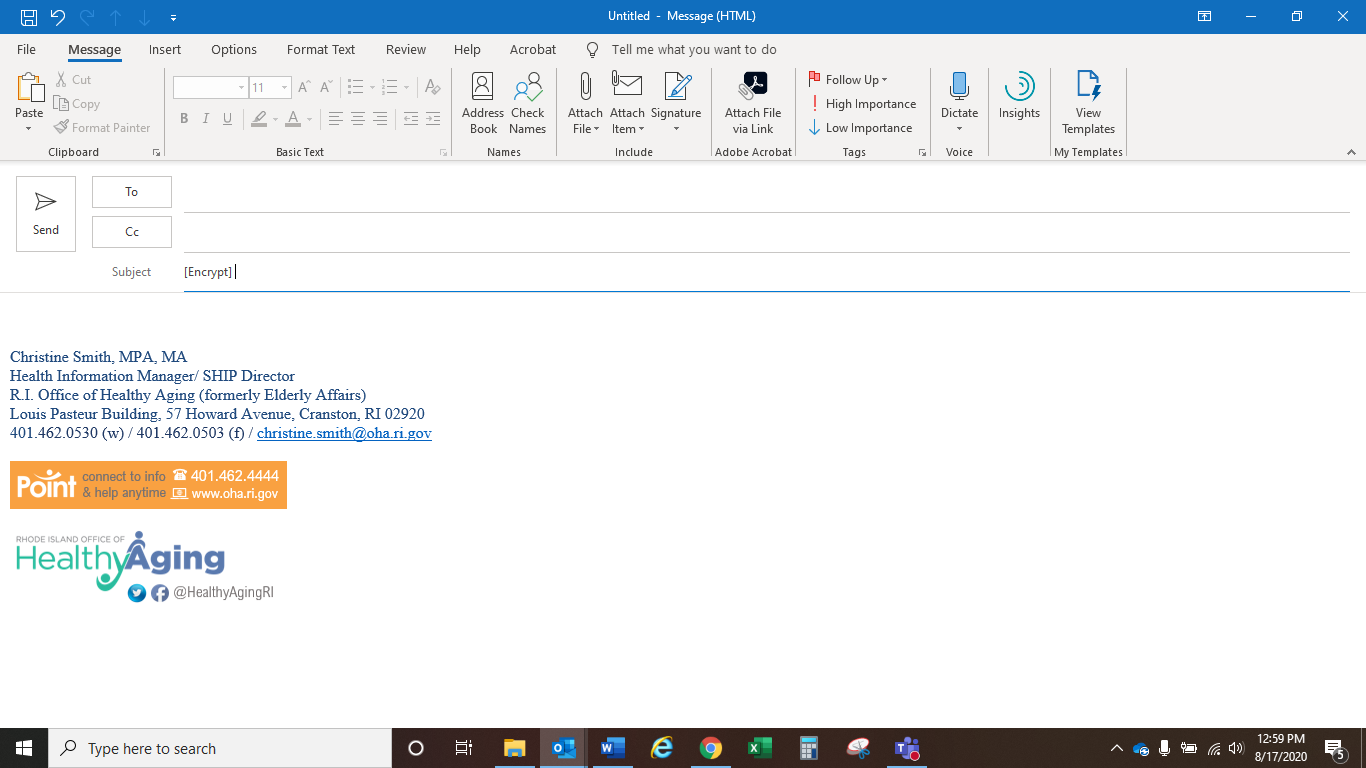
* Use the post office to mail it, or
* If the recipient has a fax machine, you can fax it.

Another option is to use a company that is able to do “print to mail.” This can be an expensive option. The average Midwest cost is around $2.30 per mailing. Here are some parameters that can be given by an ACL grantee to a “print to mail” service:

* Completed cost comparisons would be emailed to the vendor, and the average number of pages would be 11 (single-sided).
* Vendor would also be sent a formatted cover letter that provided beneficiary name, address, and key points for the beneficiary to review in their cost comparison.
* Documents would need to be printed, stuffed in an envelope, and mailed first class.
* Mailings needed to be sent and processed at least twice per week.

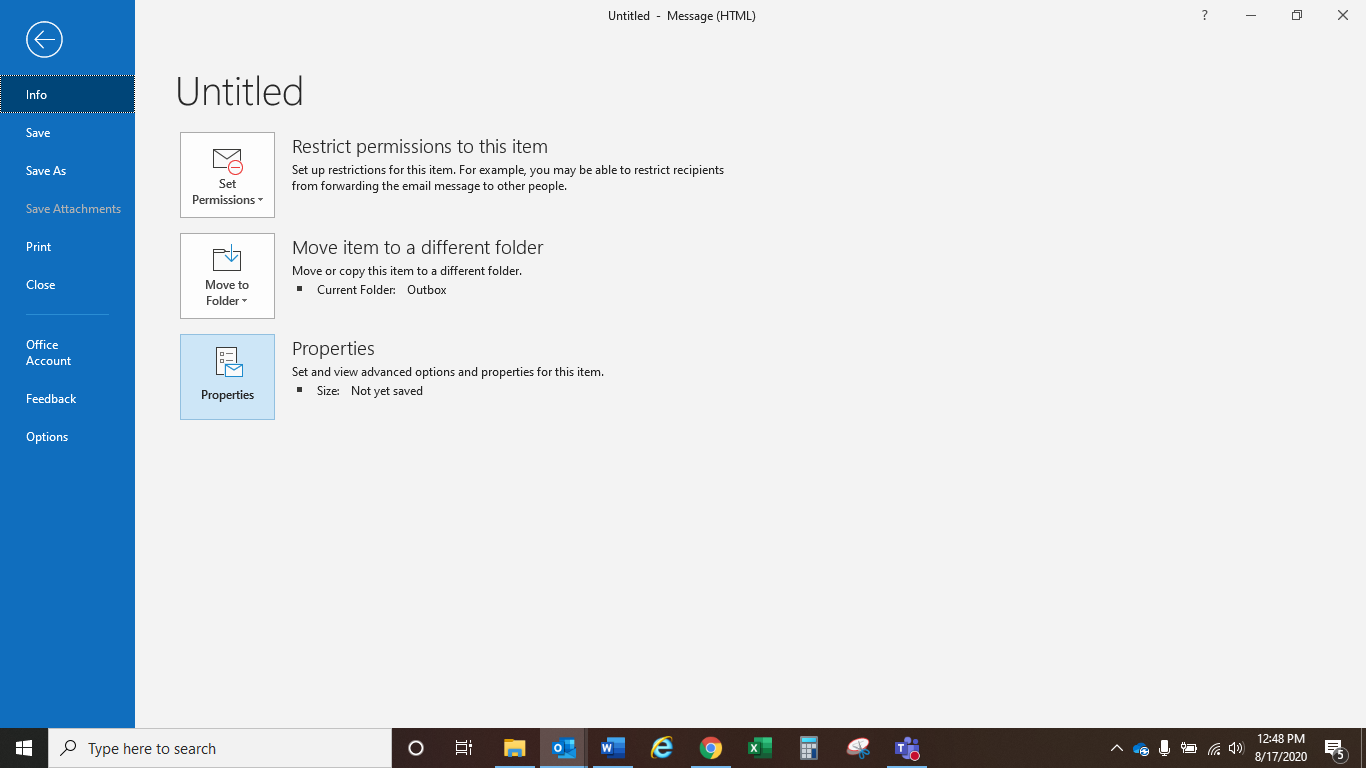
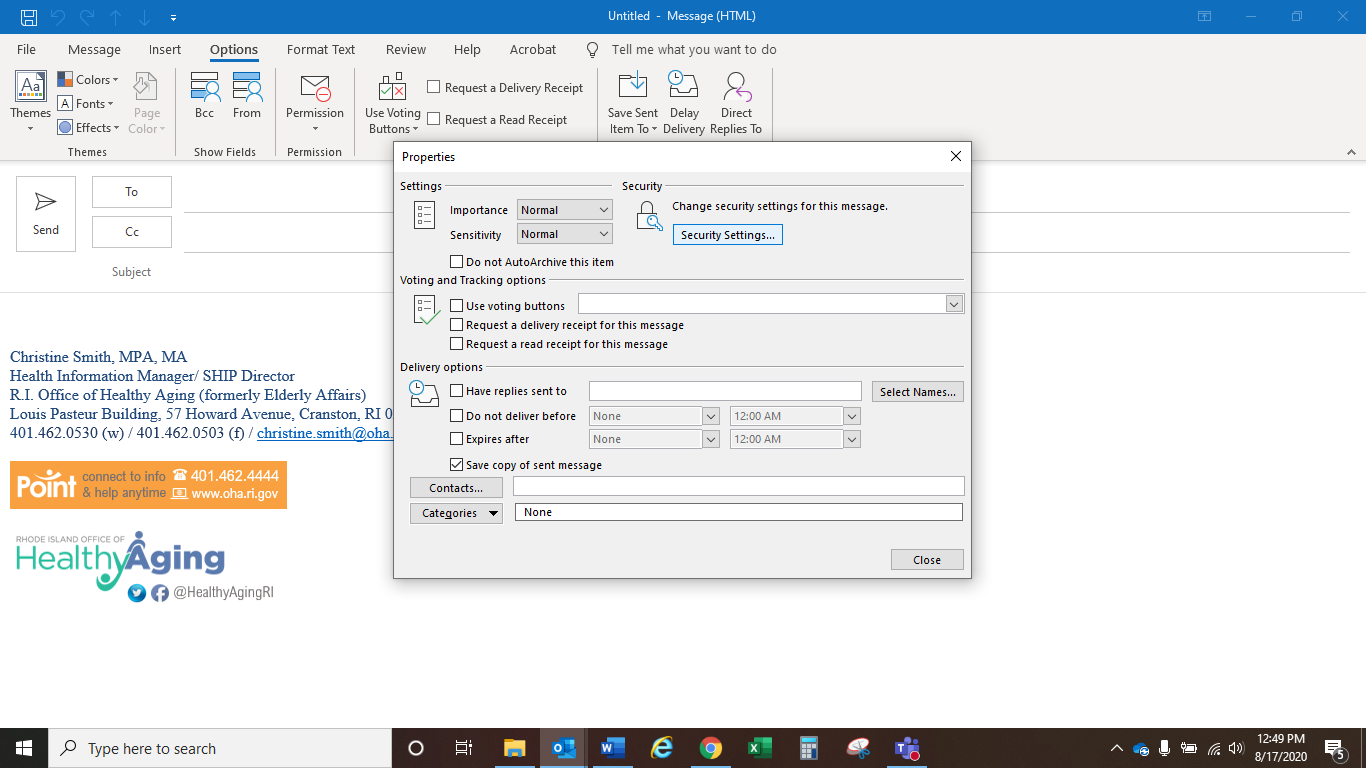
# Using Microsoft Outlook to Send Confidential Emails

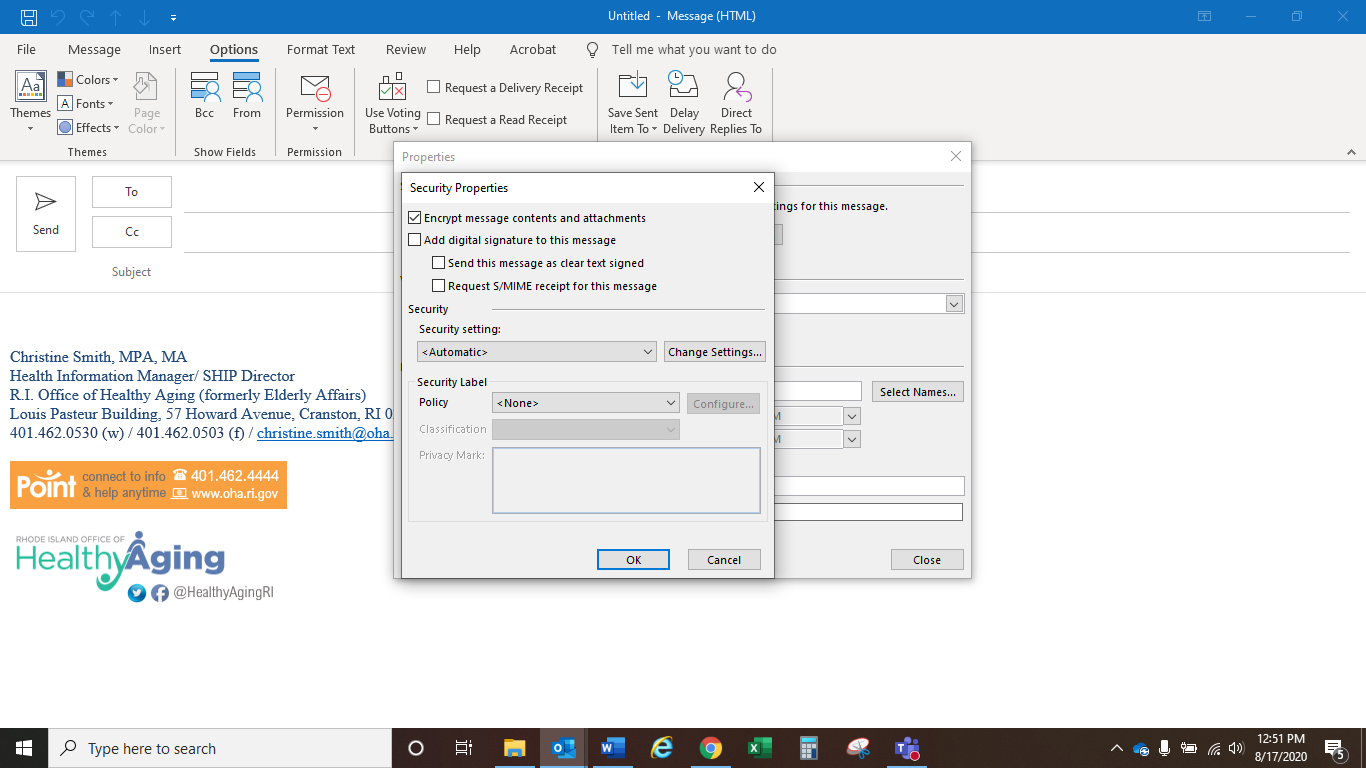
### Microsoft Office: Encrypt by Subject Line

1. Compose a new email.
2. Use **[Encrypt]** as the first word in your subject line, including the brackets, as shown below. This will automatically signal Outlook to send the message as an encrypted message. 

**Tip:** For more information on how recipients will open the messages, see the [Microsoft Office: Receiving Confidential Emails](#_Microsoft_Outlook:_Receiving) section.

### Microsoft Office: Encrypt a Single Message

1. Compose a new email.
2. In message that you are composing, click the “File” tab and then select “Properties.”
3. Click the “Security Settings” button.



1. Under Security Properties, click the box in front of “Encrypt message contents and attachments.”
2. Click “OK.” The message is now encrypted, and you can compose the message as normal.

**Tip:** For more information on how recipients will open the messages, see the [Microsoft Office: Receiving Confidential Emails](#_Microsoft_Outlook:_Receiving) section.

### Microsoft Office: Key Points When Using Encryption

**Replying or Forwarding**

* Your ability to reply to or forward an encrypted message depends upon the sending organization's policies. If you do not see a **Reply**, **Reply All**, or **Forward** link, it is because the sender of the message cannot allow recipients to reply to or forward the message.
* When you reply to a message, your reply will be sent securely.

**Adding Recipients**

* The ability to add or edit the recipient list when you reply to a message depends upon the sending organization's policies. The **To** and **CC** recipient fields will either be fixed so that you cannot change them, or you will be allowed to add or delete recipients from these fields. Separate multiple recipients with a comma.
* When you forward a message, you can always edit the recipient list.

**Note:** The sender's organization has the option to restrict secure messages to specific domains. If this is the case, you will see an error message if you try to forward a secure message to a recipient that is not allowed to receive it.

**Send me a copy**

* Proofpoint Encryption does not automatically place a copy of a secure message in your *Sent* folder. Click **Send me a copy** when you forward or reply to a secure message so that a copy will be sent to your address for your records.

**Adding an Attachment to Encrypted Email**

* If you want to add an attachment to a message, click the **Attach a file** link. Navigate to the file you want to attach and then click the **Add** link. The name of the attached file displays in the dialog box. Click **Upload** when you are done adding attachments.
* To delete an attachment from a message, click the **X** link to the right of the attachment.

**Note:** The (combined) attachments cannot exceed 15 MB in size.

**Resetting Your Expired Password**

* Your email administrator can force your password to expire after a designated period of time according to your organization's security policies. You will see a "Days until password expiration" message when you read or compose a secure message. Click the link to reset your password. If your password expires before you have a chance to reset it, you will be prompted to reset your password the next time you try to compose or read a secure message.
* You may also be required to reset your password the first time you log in to Proofpoint Encryption depending on how your account was initially set up by the administrator. Or, if you forgot your password and your administrator gives you a new temporary password, you will be required to reset it and select new security questions.

**Reading a Secure Message on a Smart Phone**

* Various smart phones cannot download files, and some smart phones modify HTML files. Since your secure message is sent to you as an HTML attachment, you may not be able to read it on your smart phone. If you have trouble reading your secure message, follow the instructions to forward the message to another server. You will then be able to download the message from the server to read it.

**Troubleshooting Error Messages**

* **You authenticated successfully, but do not have permission to decrypt this message.**  
  You do not have permission to decrypt this message. Or, the administrator has disabled your ability to decrypt the message. Contact your email administrator.
* **You authenticated successfully, but the decryption key for your message has been deleted.**  
  The decryption key for this message has expired or has been deleted. Contact your email administrator.
* **There was a critical error processing your request. There may be a problem with the system or your request.**  
  Proofpoint Encryption is temporarily unavailable. If this situation persists, contact your email administrator.
* **The message you are trying to read is corrupted and cannot be processed. Please contact the sender of the message.**  
  The message is corrupted and cannot be decrypted. Contact the sender of the message.
* **The page you requested was not found. If you clicked a link to get here, click the Back button in your browser to return to the previous page.**  
  The page you are trying to view in the browser is not available or does not exist. Click the Back button in your browser.
* **The username you requested has already been registered.**  
  You have already authenticated with Proofpoint Encryption.
* **There was an error retrieving the key for your message. If this error persists, please contact your administrator.**  
  The key server is temporarily unavailable. Try again later, and if you still cannot decrypt the message, contact your email administrator.
* **Your account has been disabled.**  
  Your email administrator has disabled your account.
* **Login Disabled**  
  You do not have permission to perform this action.

### Microsoft Office: Additional Troubleshooting Concerns

**Error with Large HTML Secure Messages**

* If your HTML message contains more than 500 KB of content, you may encounter a "Large Message Warning" error message. This limitation applies to Firefox 3.X or Internet Explorer browsers when you reply to the message or forward it. This limitation does not apply to plain text.

**Intermittent Problem with Replying to or Forwarding Secure Messages**

* If Proofpoint Encryption hangs when you try to compose a message and click the Reply, Reply All, or Forward links, click Cancel and try again. If the original text of the secure message does not display in the browser, refresh the browser or close the browser and open it again. The behavior is infrequent, intermittent, and typically works the second time around.

**If you use Outlook 2007 on Windows Vista**

* Do not save the *SecureMessageAtt.htm* attachment to disk and then try to open it. Open it from the email message.

# Using Gmail to Send Confidential Emails

You can send messages and attachments with Gmail's confidential mode to help protect sensitive information from unauthorized access. You can use confidential mode to set an expiration date for messages or revoke access at any time. Recipients of the confidential message will have options to forward, copy, print, and download disabled.

**Note:** Although confidential mode helps prevent the recipients from accidentally sharing your email, it doesn't prevent recipients from taking screenshots or photos of your messages or attachments. Recipients who have malicious programs on their computer may still be able to copy or download your messages or attachments.

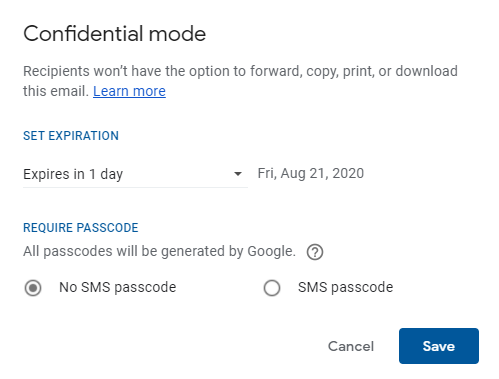
### Gmail: Creating a Confidential Email

1. Click the “Compose” button to start a new email.
2. In the bottom right of the window, click Turn on confidential mode by clicking this button Turn on confidential mode.



**Tip:** If you've already turned on confidential mode for an email, go to the bottom of the email, then click Edit.

1. Set an expiration date and passcode. These settings impact both the message text and any attachments.
   * If you choose "No SMS passcode," recipients using the Gmail app will be able to open it directly. Recipients who don't use Gmail will get emailed a passcode.



* + If you choose "SMS passcode," recipients will get a passcode by text message. Make sure you enter the recipient's phone number, not your own.

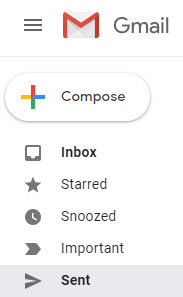
1. Click “Save.”



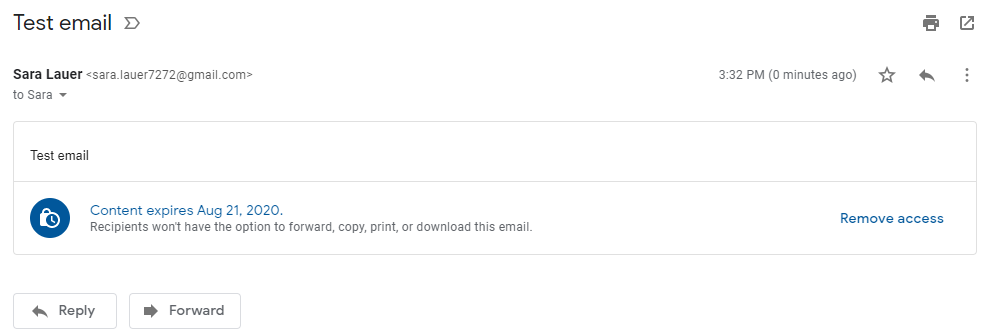
1. The email will appear like the message on the right. Compose the message as normal.

**Tip:** For more information on how recipients will open the messages, see the [Gmail: Receiving Confidential Emails](#_Gmail:_Receiving_Confidential) section.

### Gmail: Remove Access Early to a Confidential Email

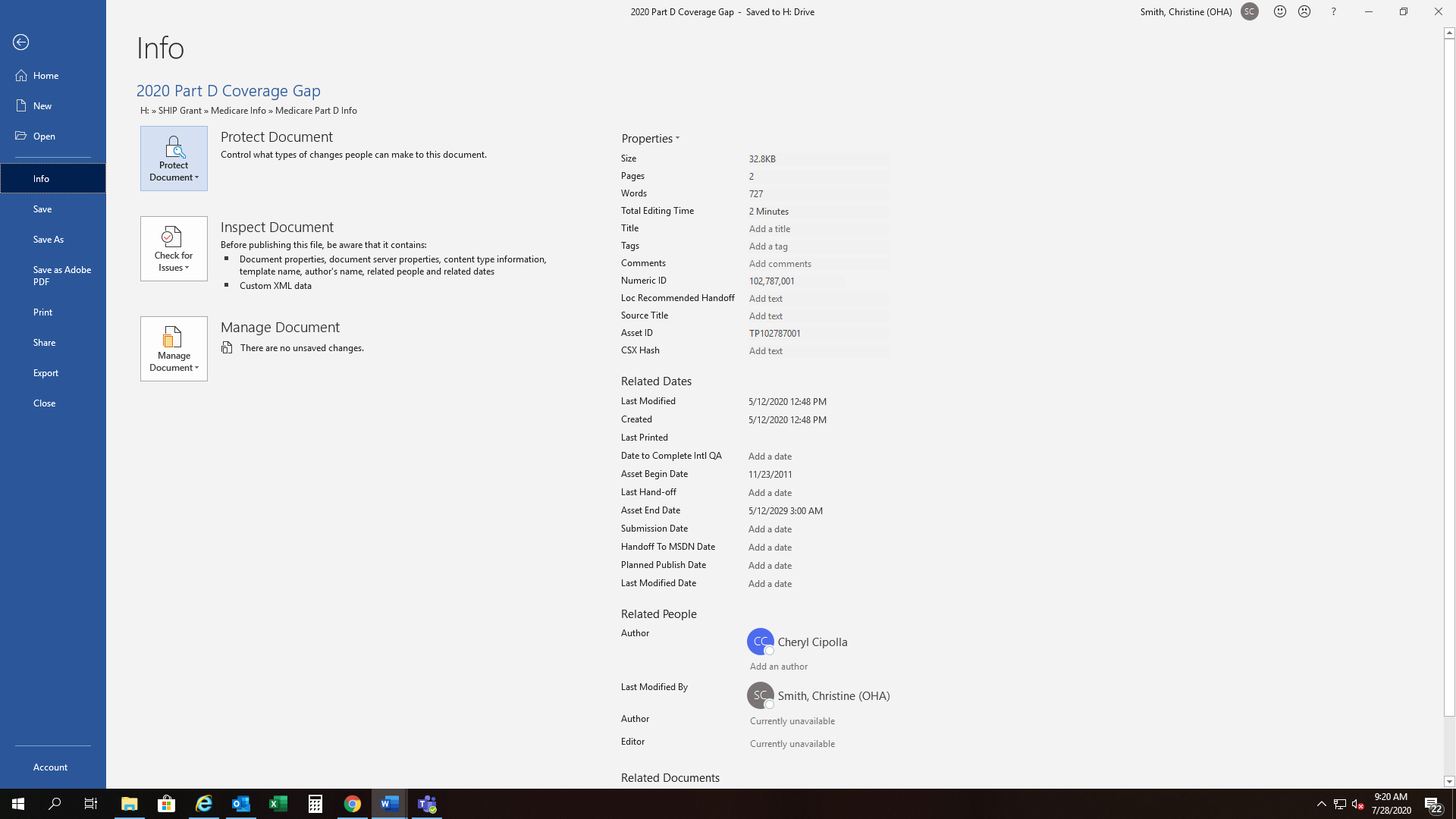
You can stop your recipient from viewing the email before the expiration date.

1. Open Gmail.
2. On the left, click the “Sent” link.
3. Find the confidential email and double click on it to open the email.
4. Click “Remove access” on the right side of the email.

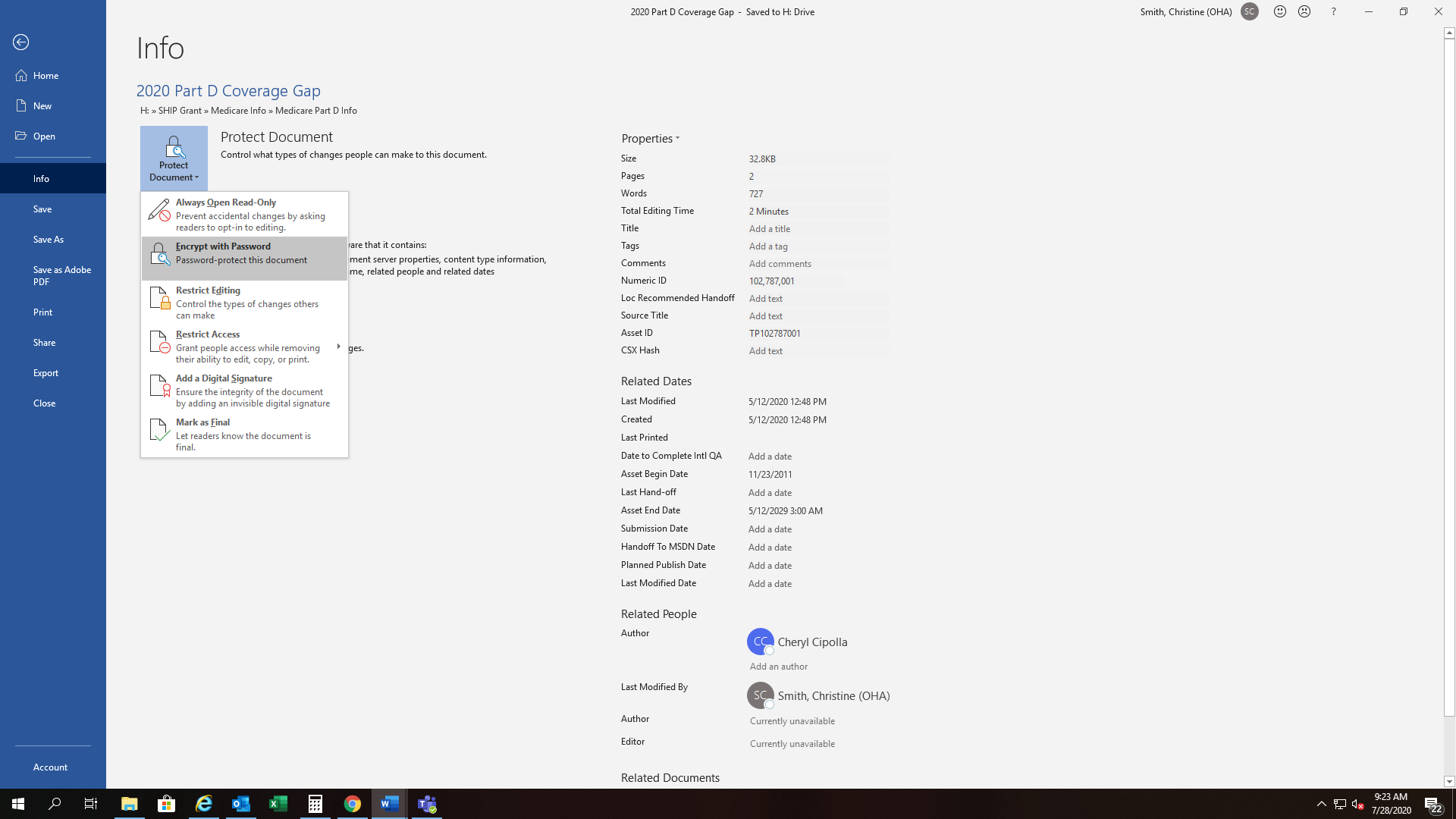


# Creating a Microsoft Word Password-Protected Document

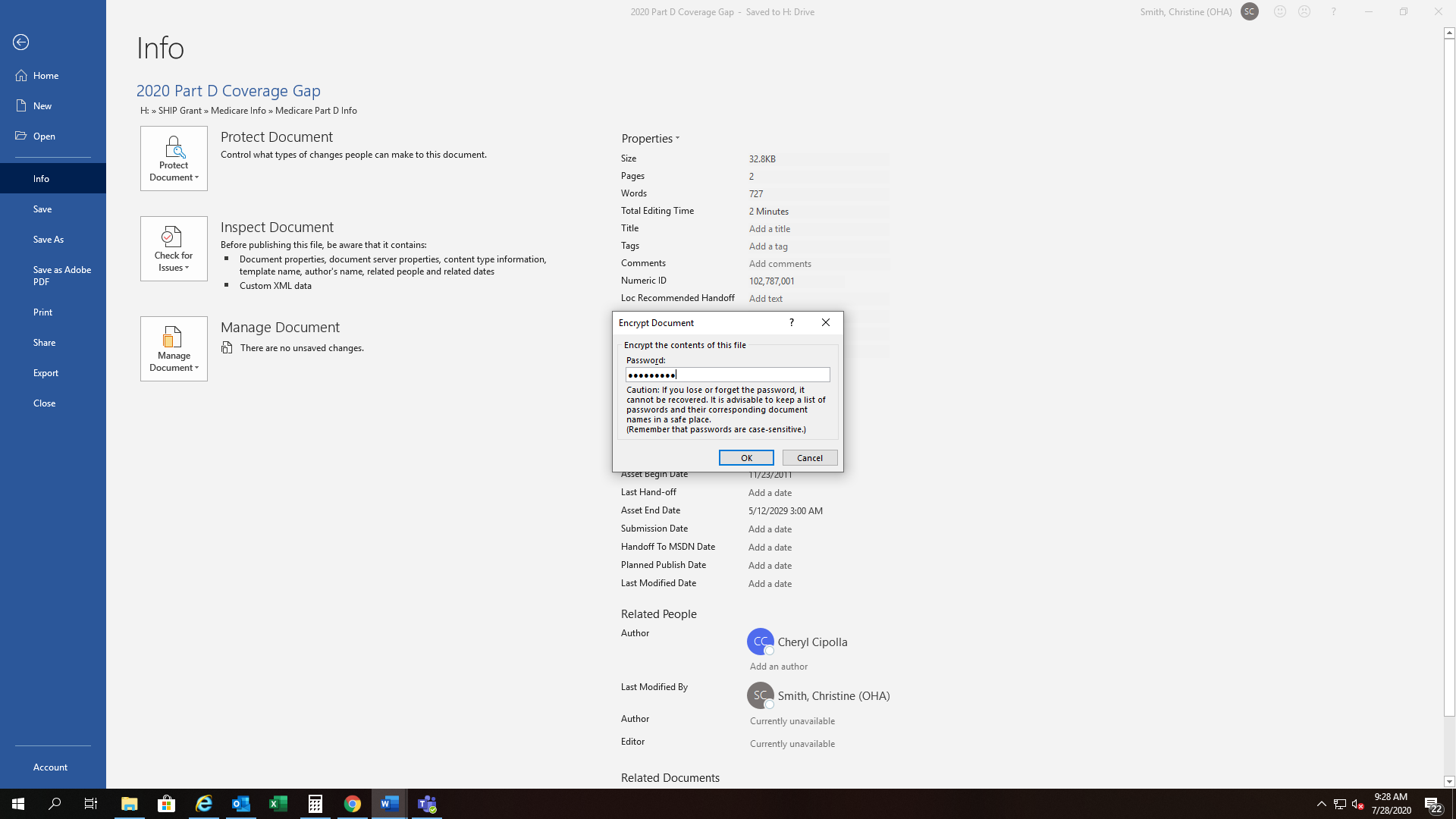
### Microsoft Word: Creating a Password-Protected Document



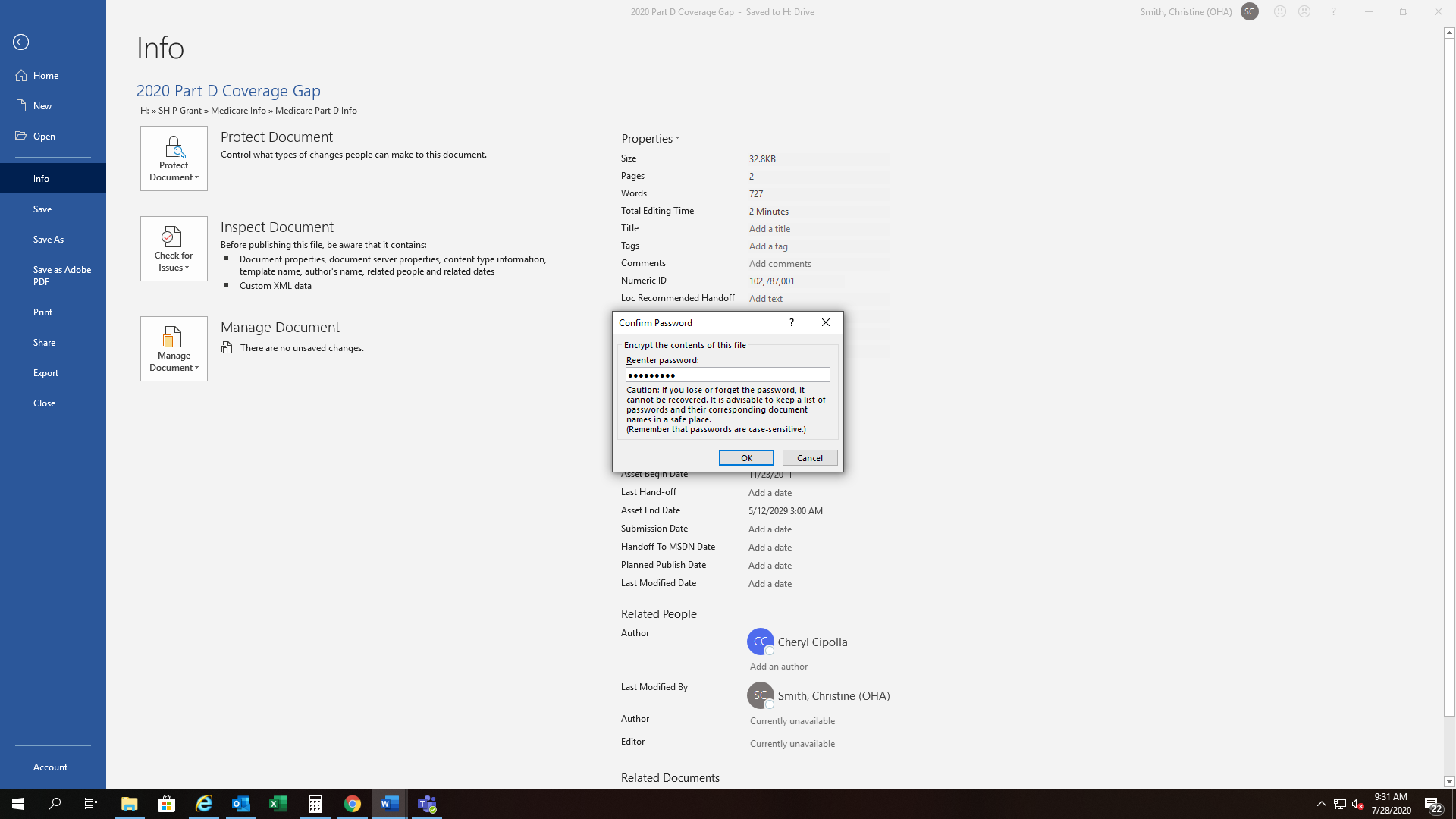
1. Open a word document in Microsoft Word.
2. Click the “File” tab and then select the “Info” section.
3. Click the “Protected Document” button to open the dropdown and then select “Encrypt with Password.”

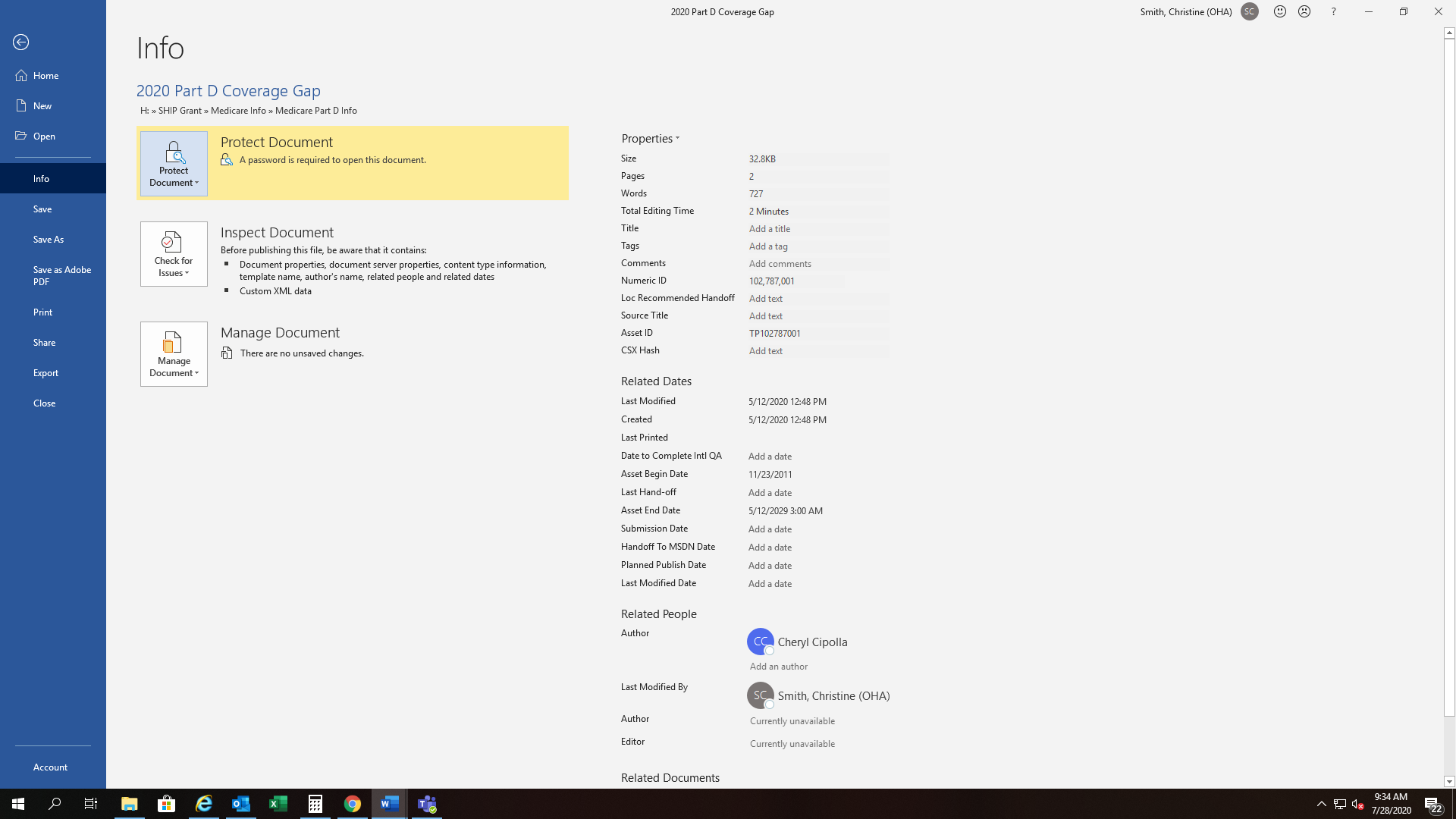


1. In the Encrypt Document pop-up type a password, and then click “OK.”



1. In the Confirm Password pop-up, reenter the password again, and then click “OK.”

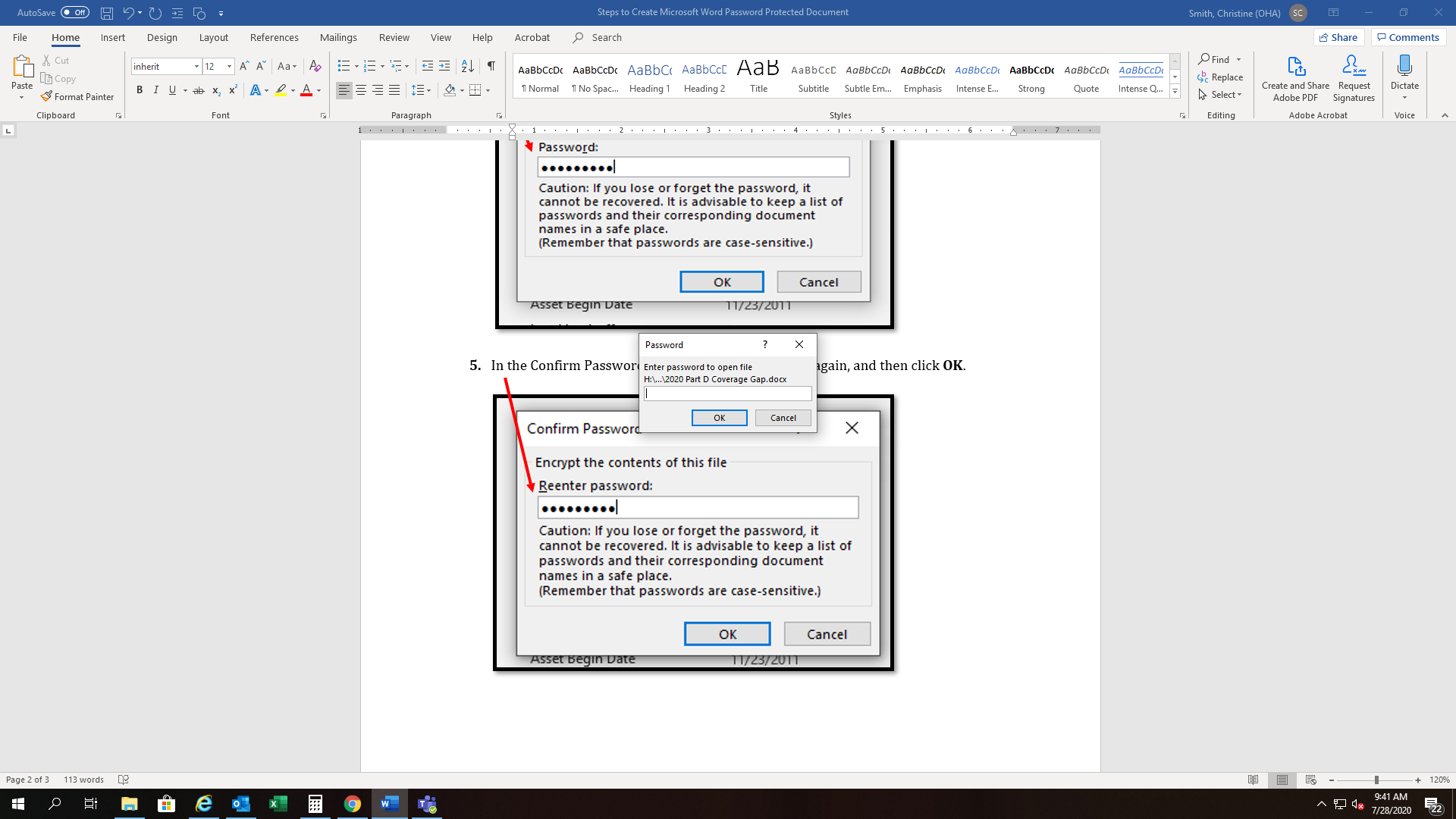
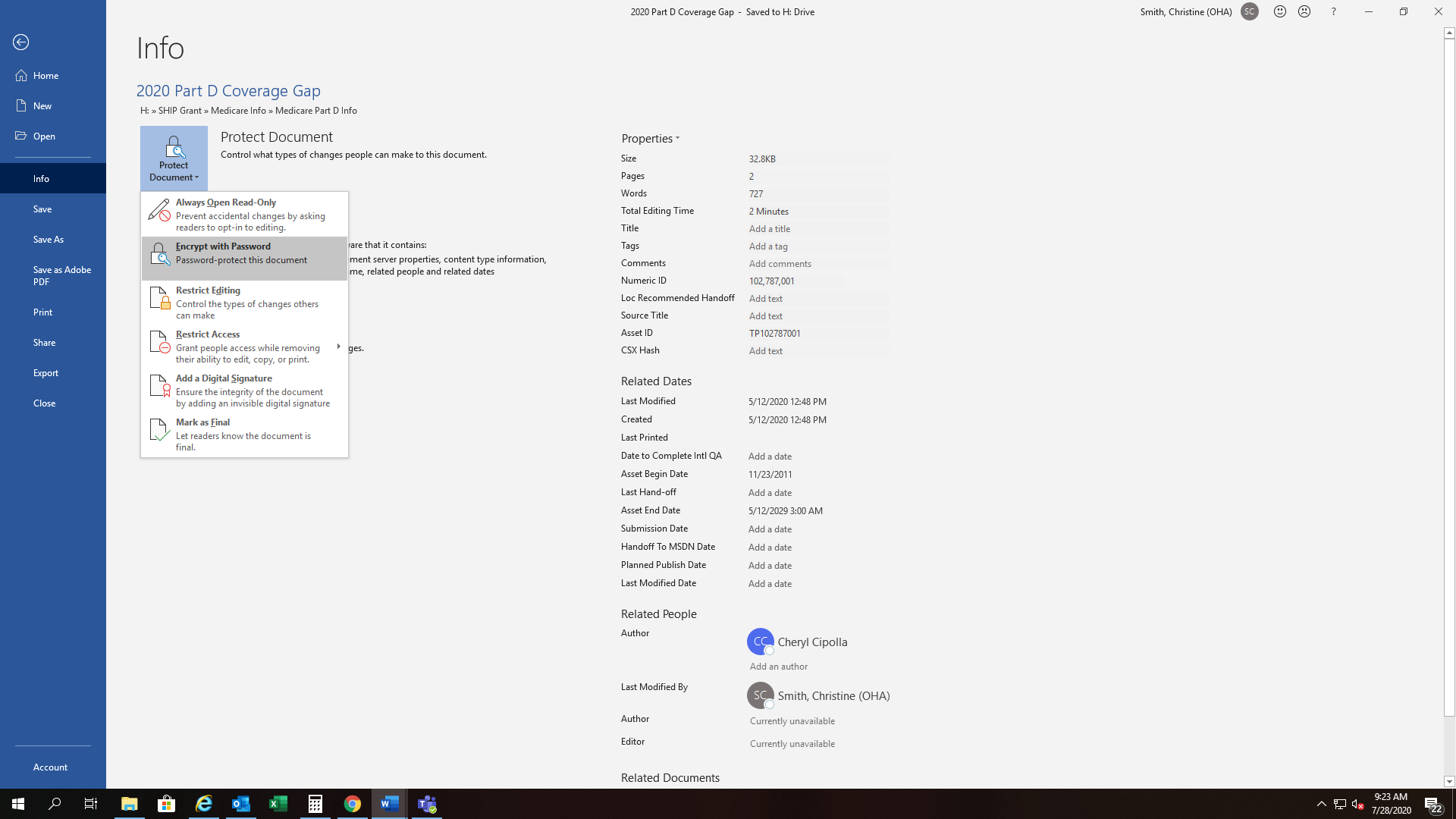
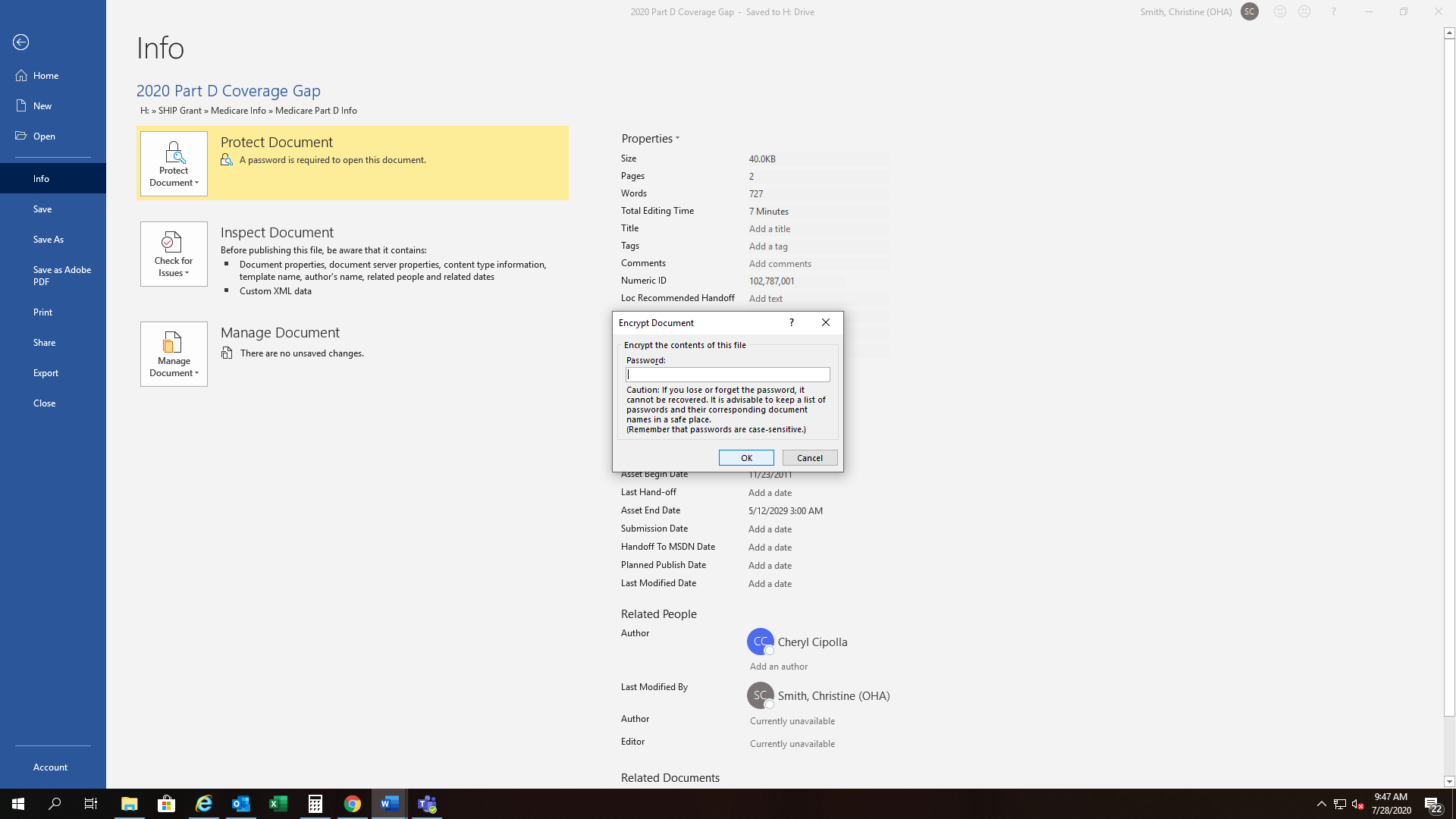




1. If the password was accepted, your word document will then display “A password is required to open this document” under the Protect Document heading.
2. Attach the document to your email. Call the recipient to give them the password over the phone or send it in a separate email.

**Tip:** For more information on how recipients will open a protected Microsoft Word document, see the [Microsoft Word or Adobe PDF: Receiving a Password-Protected Document](#_Microsoft_Word_or) section.

### Microsoft Word: Remove Password-Protected Security

1. Open the document and enter the password that was created.
2. Click on the “File” tab, then click the “Info” link, then click the “Protect Document” button, and select “Encrypt with Password” from the dropdown.
3. Clear the password in the Password box,   
   and then click OK.
4. The Protect Document will no longer appear highlighted nor will it indicate that a password is required to open the document.

# Creating an Adobe Acrobat Password-Protected Document

You can limit access to a PDF by setting passwords and by restricting certain features, such as printing and editing. However, you cannot prevent saving copies of a PDF. The copies have the same restrictions as the original PDF. Two types of passwords are available:

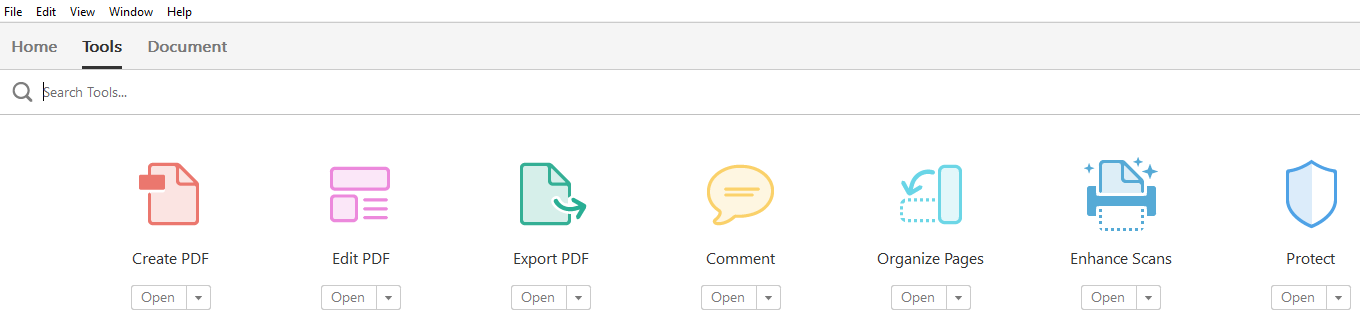
* **Document Open Password** – (also known as a *user* password) requires a user to type a password to open the PDF.
* **Permissions Password –** (also known as a *master* password) requires a password to change permission settings. Using a permissions password, you can restrict printing, editing, and copying content in the PDF. Recipients don’t need a password to open the document in Reader or Acrobat. They do need a password to change the restrictions you've set.

If the PDF is secured with both types of passwords, it can be opened with either password. However, only the permissions password allows the user to change the restricted features. Because of the added security, setting both types of passwords are often beneficial.

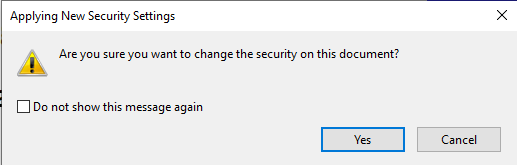
**Note:** You cannot add passwords to a signed or certified document.

### Adobe Acrobat: Creating a Password-Protected PDF Document

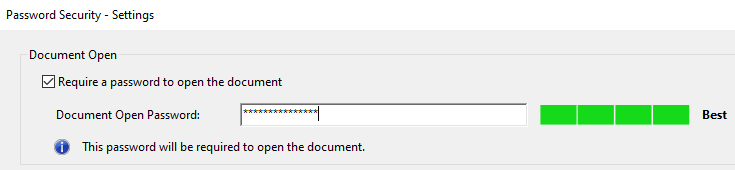
1. Open the PDF.
2. Click on the “Tools” tab, then click the “Protect” button.



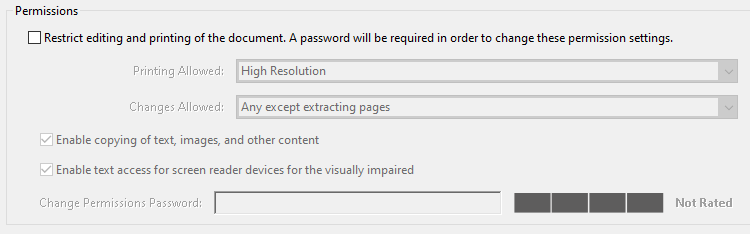
1. You are returned to the document. Click the “Encrypt” dropdown at the top of the screen and select “Encrypt with Password.”



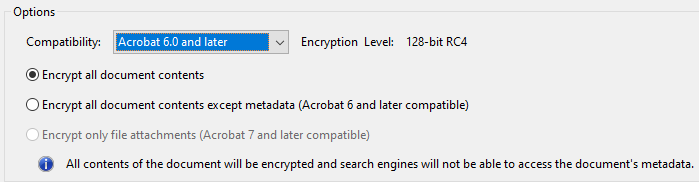
1. If you receive a prompt, click “Yes” to change the security.
2. Under Password Security – Settings, click the box in front of “Require a password to open the document,” then type the password in the corresponding field. The password strength is displayed next to your password to indicate whether the chosen password is weak, medium, strong, or best.



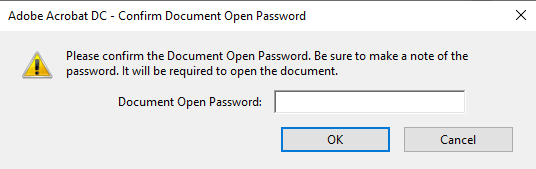
1. Under the Permissions section, make changes only if you do not want the recipient to edit or print the document.



1. Under the Options section, change the Compatibility option to be the lowest version available.

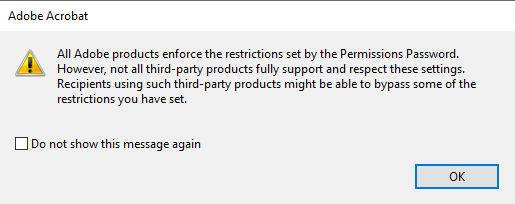


1. Click “OK” at the bottom of the pop-up.
2. Confirm the Document Open Password by retyping it in the pop-up and then click “OK.”

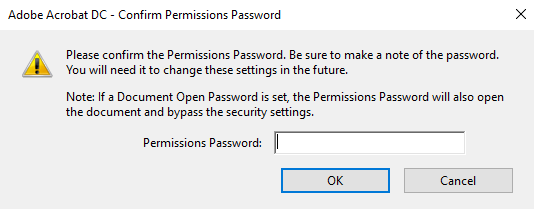


**Note:** If you also restricted editing and printing in the permissions section, you also receive the following pop-ups:

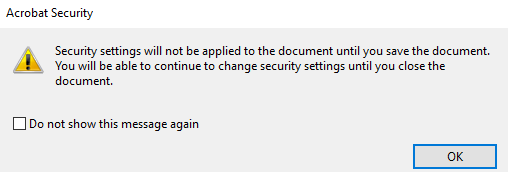
* + - Acknowledge that all Adobe products enforce the restrictions set by the Permissions Password, but all third-party products may not. Click “OK.”



* + - Confirm the Permissions Password by retyping it in the pop-up and then click “OK.” (Screenshot is on next page.)



1. Click “OK” to the following pop-up that let you know the security settings will not be applied until you save the document.



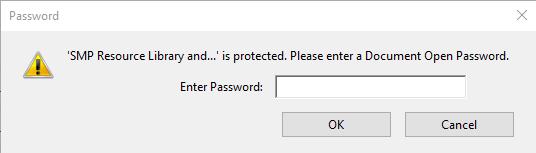
1. Save the document to save the security settings.
2. Attach the document to your email. Call the recipient to give them the password over the phone or send it in a separate email.

**Tip:** For more information on how recipients will open a protected Microsoft Word document, see the [Microsoft Word or Adobe PDF: Receiving a Password-Protected Document](#_Microsoft_Word_or) section.

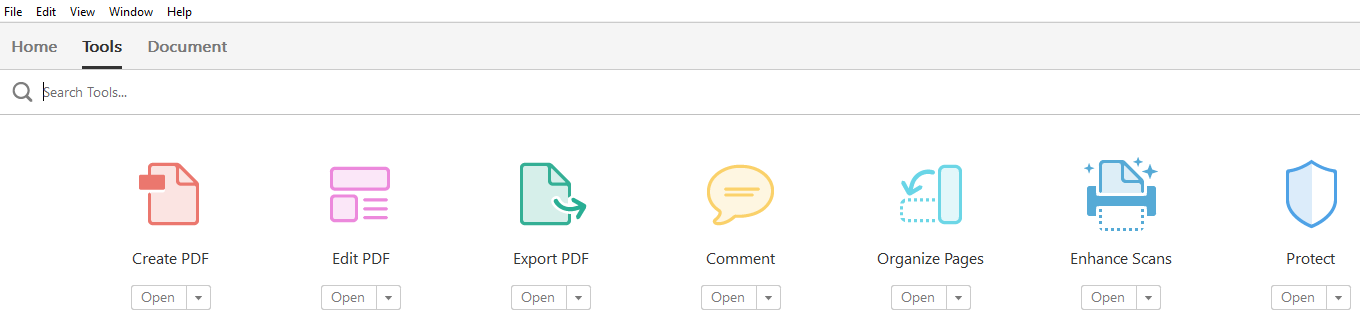
### Adobe Acrobat: Remove Password-Protected Security

You can remove security from an open PDF if you have the permissions to do so. If the PDF is secured with a server-based security policy, only the policy author or a server administrator can change it.

1. Open the PDF.
2. Enter the Document Open Password to access the document and then click “OK.”



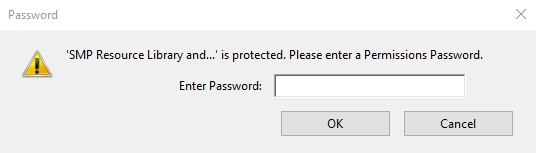
1. Click on the “Tools” tab, then click the “Protect” button.



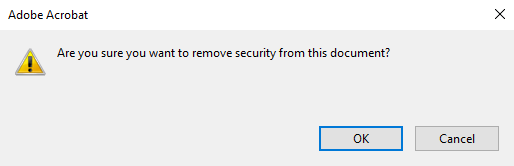
1. You are returned to the document. Click the “Encrypt” dropdown at the top of the screen and select “Remove Security.”

**Note:** If you also restricted editing and printing in the permissions section, you receive the following pop-up first:

* + - The first pop-up will have you enter your Permissions Password and then click “OK.”



1. Click “OK” to the pop-up asking if you are sure you want to remove security from the document.

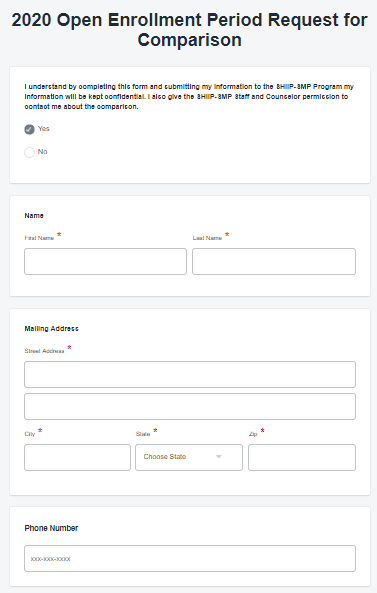
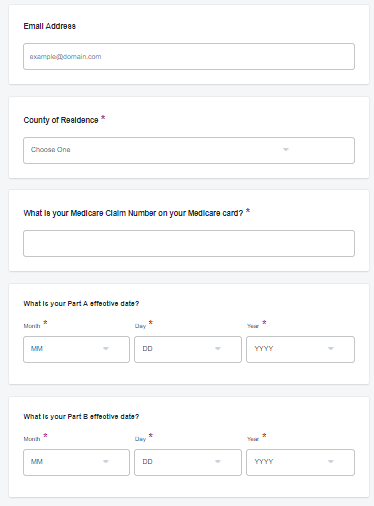


# Using Fillable Online Forms to Collect Confidential Information

A form that is web-based and can be shared via a link is a secure way to collect beneficiary information. Listed below are a few HIPAA compliant companies that offer online form services. The producers of this toolkit do not recommend any specific vendor, nor does the U.S. Administration for Community Living (ACL). This list is not exhaustive and is provided simply as a starting point.

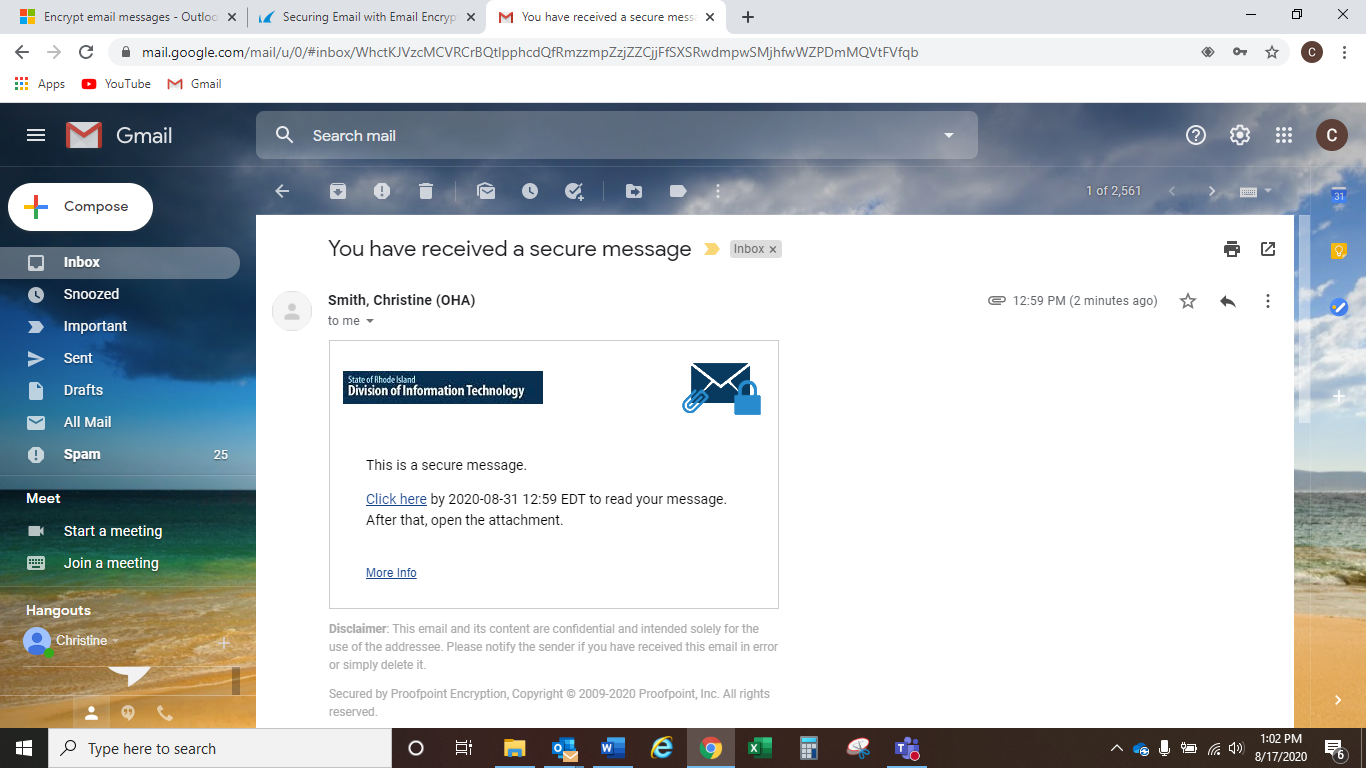
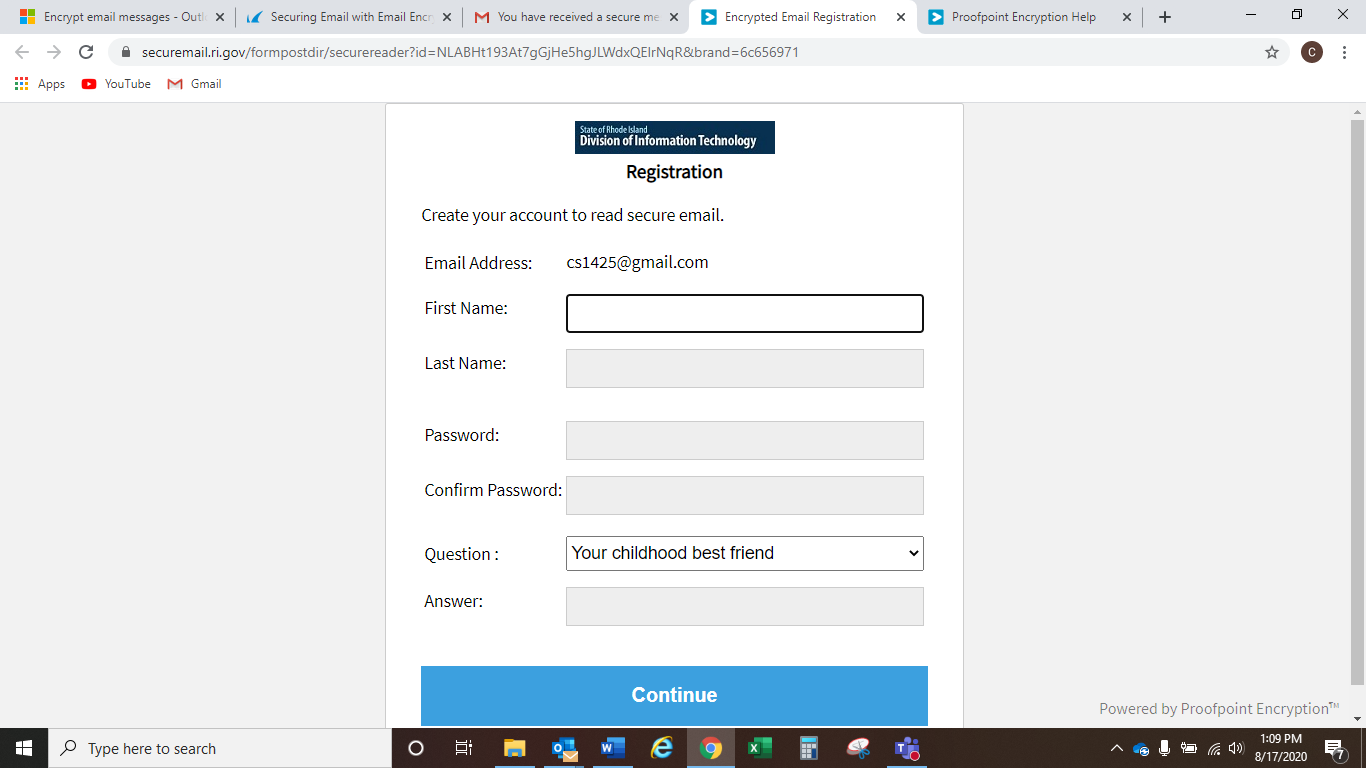
|  |  |  |  |
| --- | --- | --- | --- |
| Option | Details | Cost | Link |
| LUXSC | Base package offers 25 unique forms for you to publish and up to 5,000 submissions per day | $50.00 a month | <https://luxsci.com/package-levels.html> |
| JotForm | 10,000 monthly submissions, up to 100 forms, unlimited fields | $29.00 a month | <https://www.jotform.com/pricing/> |
| Hushmail | Up to 10 webforms and 10 secure email accounts | $39.00 a month | <https://www.hushmail.com/business/healthcare/hipaa-compliant-email/?source=website&tag=page_business,sidebar_menu> |
| SeamlessDoc | Operates at state government level | Quote needed | <https://seamlessdocs.com/> |

### Fillable Online Form: Example



# Beneficiaries and Receiving PPI Guidance

### Microsoft Outlook: Receiving Confidential Emails

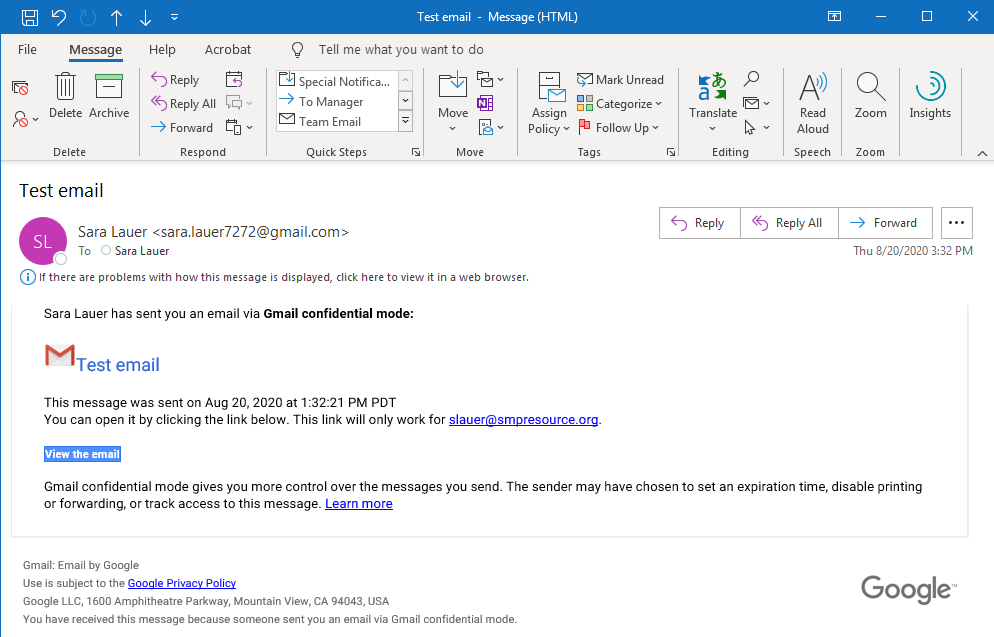
1.  A counselor will send you an email that will appear like the following. Once received, click on the “Click Here” link to open the message.
2. You will be bought to the following screen.
   * If you have already registered, or if your account already exits, you will be prompted to sign in and enter your password to decrypt the message. Click “Continue.”
   * If you have not registered for Proofpoint Encryption, you will be prompted to create an account and choose a password on the Registration page. Click “Continue” when you are done. In the future, you will not be prompted to register.

**Note:** If you sign in, and the Login screen returns with a field that you can edit for your username, it means Proofpoint Encryption found a record for you, but the email address is different - perhaps an email alias. Enter a different address to sign in. For example, a record for jsmith@example.com exists, but you entered joe@example.com - your alias for jsmith.

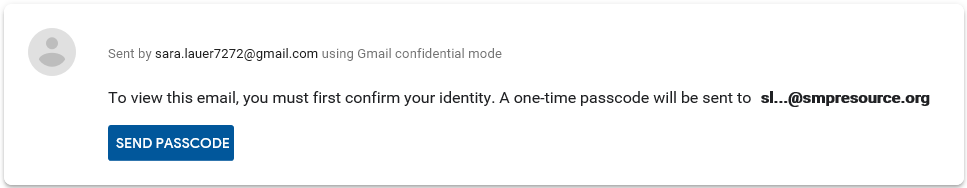
**Tip: Forgot your password?** If Proofpoint Encryption is configured to allow you to reset your password, click the Forgot Password link. You will be prompted for your security question. Create a new password for your account.

### Gmail: Receiving Confidential Emails

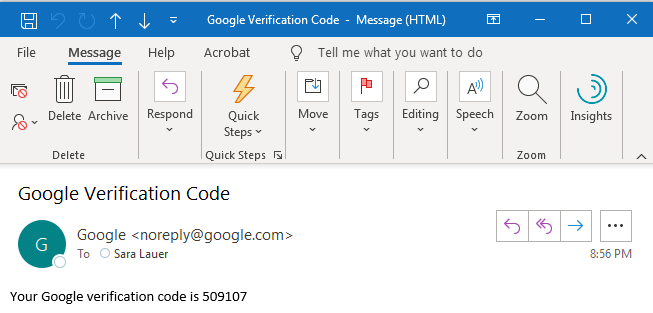
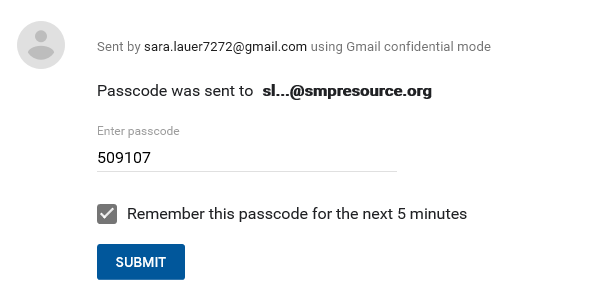
1. A counselor will send you an email that will appear like the following. Once received, click on the “View the email” link to open the message.



1. To view the email, you must first confirm your identity. Click the “Send Passcode” button.



**Note:** If you are accessing the email using the Gmail app (mobile or desktop), you will not be asked to confirm your identity and the message will automatically open instead.

1. You will receive an email with the verification code.
2. You will then need to enter the code from the email into the verification pop-up in the “Enter passcode” field and click then click the “Submit” button.

**NOTE:** Because the sender used the confidential mode to send the email:

* You can view the message and attachments until the expiration date or until the sender removes access.
* Options to copy, paste, download, print, and forward the message text and attachments will be disabled.
* You might need to enter a passcode to open the email.

### Gmail: Error Messages

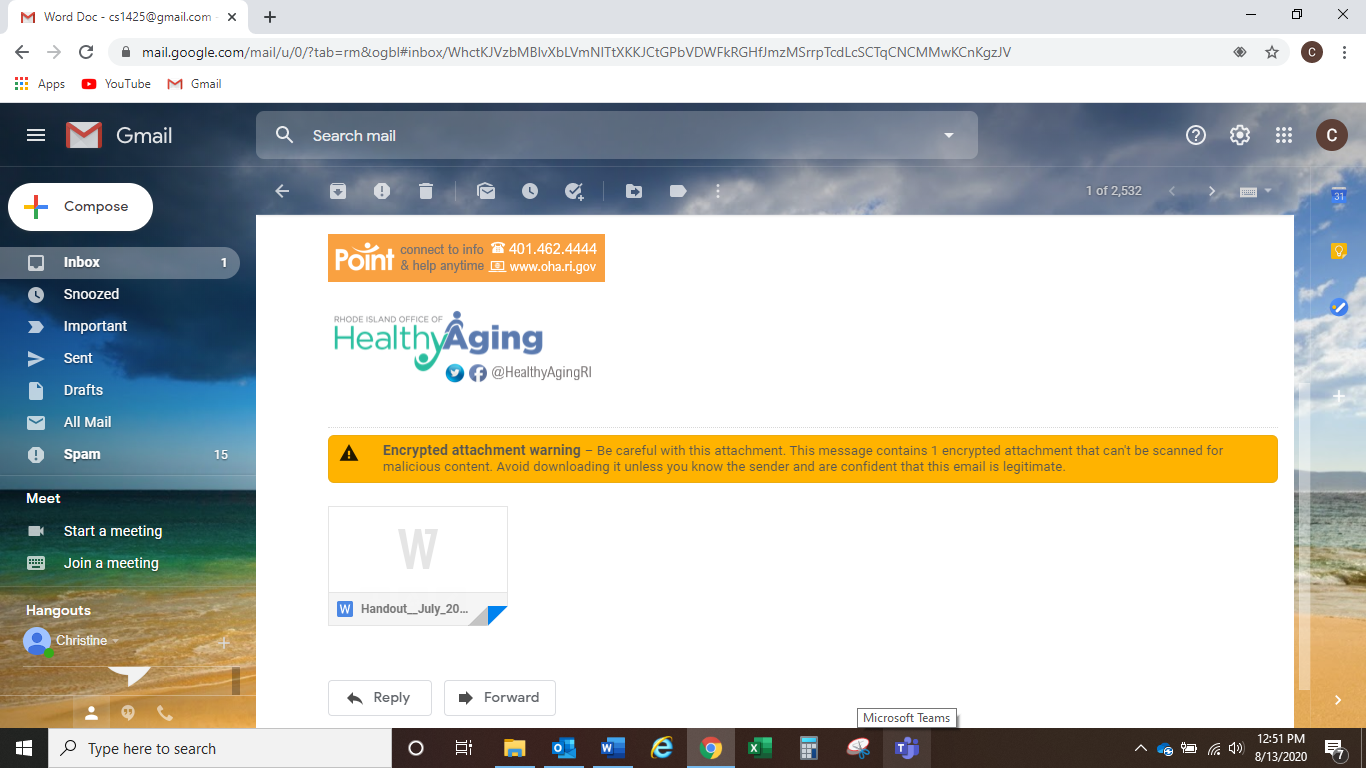
* **Email has expired -** The sender might've deleted the email or removed your access before the expiration date. Contact the sender to give you more time or to resend the email.
* **Switch accounts -** Make sure you're signed into the correct Google Account that's associated with the recipient email. Then, try to open the email again.
* **Provided number is for an unsupported country -** You can only add SMS passcodes for phone numbers from these regions: North America; South America; Europe; Australia; Asia: India, Korea, and Japan.

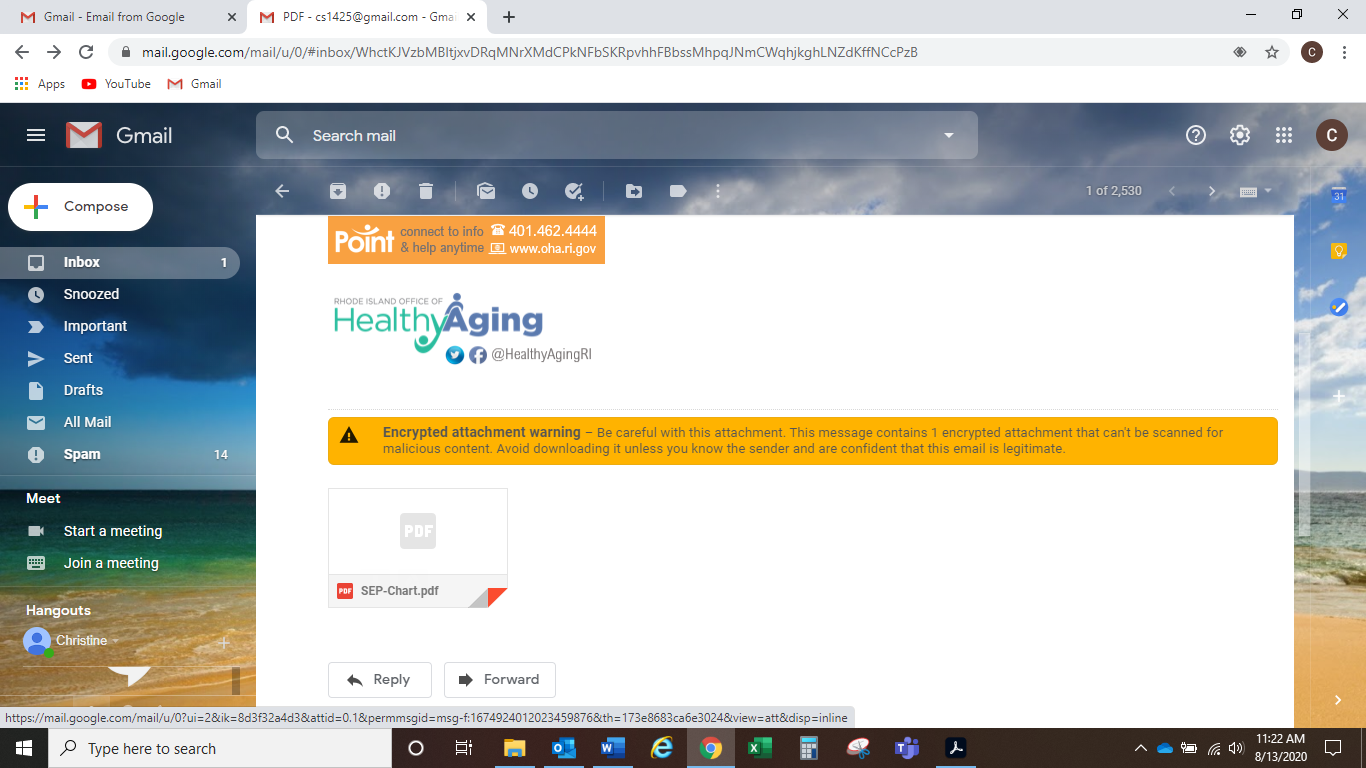
### Gmail: Additional Notes

Because the sender used the confidential mode to send you an email:

* You can view the message and attachments until the expiration date or until the sender removes your access.
* Options to copy, paste, download, print, and forward the message text and attachments will be disabled.

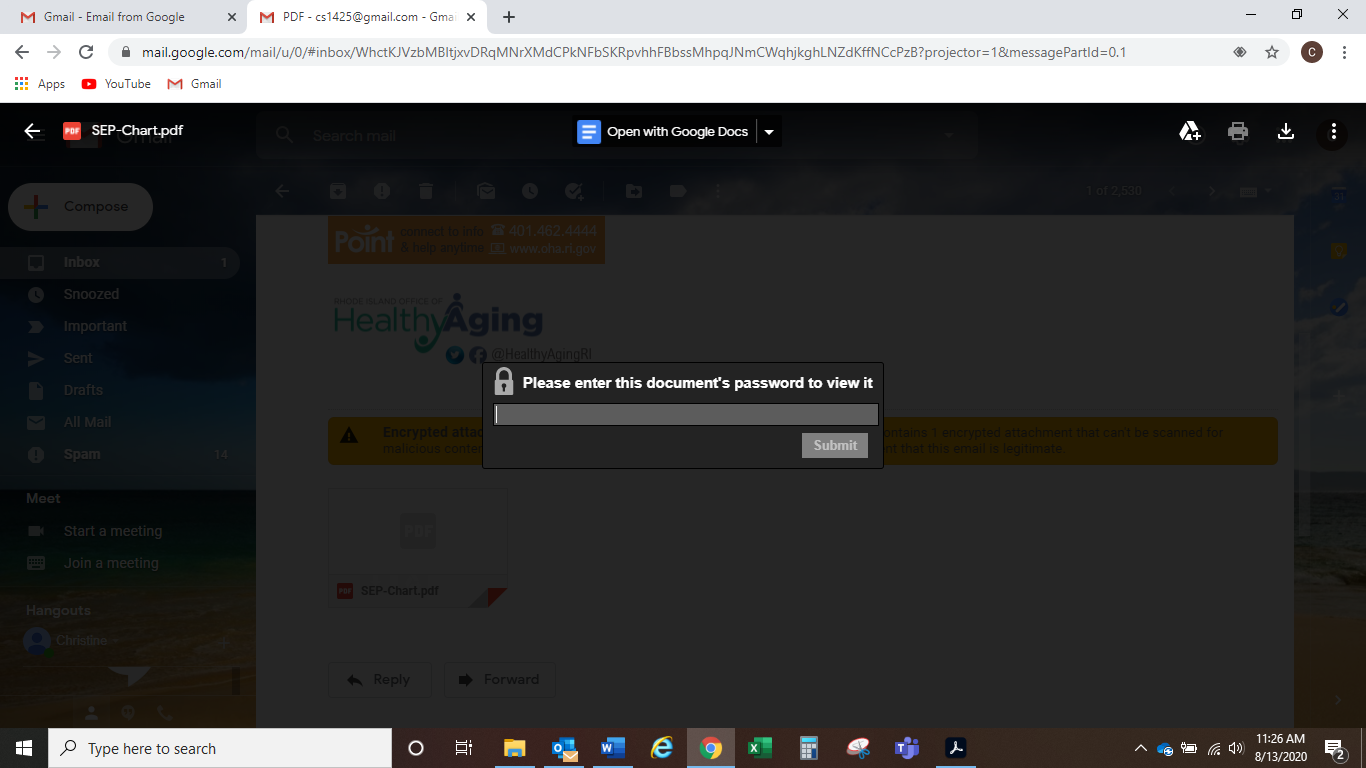
### Microsoft Word or Adobe PDF: Receiving a Password-Protected Document

1. When a counselor sends a password-protected Word or PDF document as an attachment to an email, you will see a warning message similar to these from Gmail. This just lets you know the attachment is encrypted. 



1. You will need a password to view the attachment. You will receive the password in one of two ways.
   * + The counselor will call you and tell you the password over the phone
     + The counselor will send you a separate email with the password in it

**Note:** If you do not receive the password, reach out to the counselor to have the resend it to you.

1. Once the email is received, open the attached Word document. You will receive the following pop-up. Enter the password in the open field and then click “Submit” to open the Word document.