# **Encryption Guidance**

January 2021



### CAVEATS

There is a great variety of encryption methods available depending on your computer configuration; this guide does not cover every single method available and many of you have found your own solutions.

We recognize this guide offers limited solutions and there are frequent issues with encryption tools. As a result, we are advocating and working for more sophisticated encryption tools. This guide is an important first step in demonstrating the critical need to protect University data.

Contact the appropriate compliance partner (e.g. Export Control or HIPAA) for guidance on the encrypting level requirements in the regulations. For technical assistance contact your Unit's IT Manager or the 24/7 IT Support Center.

# Topics covered

- Email
- Drives
- Documents
- File Folders
- Stache
- UA Box Health
- Questions?



### Digital Signature vs. Encryption

Encryption scrambles data to protect it and reduce the ability of unauthorized parties to understand the information.

Digital signatures bind the identity of the message sender to the message, ensuring integrity, messages authentication, and non-repudiation, whereas encryption provides confidentiality.

Use of digital ssignature may prevent encryption.



# Why is Encryption Important?

- Legally required for data subject to HIPAA and export control regulations
- Makes information more difficult to intercept and steal
- Following the requirements prevents significant fines

In 2019, The University of Rochester Medical Center (URMC) was fined \$3 million by The Department of Health and Human Services' Office for Civil Rights (OCR) for failing to encrypt mobile devices and other HIPAA violations.

https://www.hipaajournal.com/lack-of-encryption-leads-to-3-million-hipaa-penalty-for-new-york-medical-center/



# **Encrypting Email**



# EMAIL CAVEATS

- **Always send an encrypted test message before sending restricted** data to ensure the tool is properly working.
- **Do Not E-mail Controlled Unclassified Information (CUI).**
- CUI needs to be shared and contained in the S3 bucket.
- Do not use your student or personal Gmail to send encrypted **export control or HIPAA files.** The encryption level is not sufficient to comply with federal regulations.
- Students working on export control or HIPAA projects will need a ulletCatworks (Outlook) account to email or receive restricted data.



# **Outlook Encryption Restrictions**

#### Limitations: The following cannot encrypt

Emails with a **digital signature** 

Messages larger than 30Mb

**OneDrive for Business attachments** 

File attachments: .lnk, .exe, .com, .cmd, .bat, .dll, .ini, .pst, .sca, .drm, .sys, .cpl, .inf, .drv, .dat, .tmp, .msg,.msp, .msi, .pdb, .jar

**Folder attachments**: Windows, Program Files (\Program Files and \Program Files (x86)), \ProgramDatas, \AppData (for all users)

Microsoft Office	?	$\times$
Only file attachments that support rights management will automatically have their perestricted to match the restrictions on this e-mail. All other file types are attached unper Click Learn more to see a list of file types that support rights management.	rmission rotected	





# Sending Encrypted Email in Outlook Online (O365)

#### STEPS

- 1. Click "encrypt" at top of message, near "send"
- 2. **Confirm encryption**: message above "From": *"Encrypt: This message is encrypted...."*
- **3. Permission levels** can be changed at the end of encryption message:
  - **Encrypt**: Recipients can't remove encryption.
  - **Do Not Forward**: Message can be read, but cannot be forwarded, printed, or have its contents copied.
  - University of Arizona Confidential: Content can be modified but cannot be copied and printed.
  - University of Arizona Confidential View Only: Content cannot be modified.



Microso	ft Office Home	Mail -
lege of Pharmacy Outlook		
age	⊳ Send 🔋 Attach ∨ 🕲 Encrypt) 🗊 Discard …	
	From johnson@Pharmacy.Arizona.EDU	
	То	
e	Cc	
Change permiss Choose how recipients	can interact with this message	
College of Pharmacy College of Pharmacy	- Confidential - Confidential View Only	
Do Not Forward Encrypt		



# Sending Encrypted Email in Outlook Desktop Application

#### STEPS

- 1. Click "Options" in toolbar, select "Encrypt"
- 2. Options for encryption:
- Encrypt Only: Recipients can't remove encryption.
- **Do Not Forward**: Message can be read, but cannot be forwarded, printed, or have its contents copied.
- University of Arizona Confidential: Content can be modified but cannot be copied and printed.
- University of Arizona Confidential View Only: Content cannot be modified.





<b>⊟</b> 5 ∂ <b>≓</b>	Untitled • COP
Options	
	A · abc · · ·
BCC Zoom	Encrypt-Only
	Do Not Forward
	College of Pharmacy - Confidential College of Pharmacy - Confidential View Only

Ŧ						Untitled - Mes	sage (H
Inser	t Options	Format Tex	t Review Help	ADOBE	PDF '	Q Tell me what	you war
age	Brc	Encrypt v	C Request a Delive oting Request a Read F ins ~	ry Receipt Receipt	Save Sent Item To ~	Delay Direct Delivery Replies To	
		Set permission	n on this item			Options 15	
~	iohnson@pha	email.arizo	ona.edu (bjohnson@arizor	na.edu)	>		
		pharmacy	arizona.edu (johnson@Ph	armacy.Arizo	na.EDU) >	Encrypt-On Do Not Fon College of F College of F	ly vard 'harmac 'harmac

# Sending Encrypted Email Using Subject Line Encryption

Works with Outlook Online & Desktop App

#### STEPS

Simply type [encrypt] or [secure] in the subject line.

**IMPORTANT!** This is case sensitive and not recommended as mistakes are more likely.

<u>https://it.arizona.edu/documentation/uaconnect365</u> <u>-email-encryption</u>

#### Examples: will encrypt:

- Subject: Game day plans [encrypt]
- Subject: [secure] Game day plans
- Subject: Game day [encrypt] plans
- Examples: will not encrypt:
  - Subject: [Encrypt] Game day plans
  - Subject: Game day plans [SECURE]
  - Subject: encrypt: Game day plans
  - Subject: [secure:] Game day plans



# **Receiving Encrypted Email**

#### What do external recipients see?

- Recipients receive a message with directions to access the encrypted email.
- Upon clicking "Read the Message" they are directed to a page with two options: Sign in with Google or Sign in with one-time passcode.
- Sign in with Google allows use of Gmail account to access the message.
- Sign in with a one-time passcode asks for the recipient's email address to which a code is sent to open the email.

#### Internal recipients will see a message indicating the message is enc

Bruce Johnson & encryption test to non MS dor To: Bruce Johnson Bruce Johnson (john

Learn about message

Email encryption powered by Office

licrosoft Corporation, One Microso

message\_v4.rp

•		🖶 🏲 🗸 🖾 TML	~	
nain		■ Trash - Bruce Google 12:36 PM	BJ	
on@Pharmacy.Arizona.E	DU) has sent you a			
Read the message				
protected by Office 365	Message Encryption.			
65. Learn More Way, Redmond, WA 98	cure] Game day plans	arbox x		0.5
1	Wildcat, Wilbur - (wwild	icat) <u>via</u> emailarizona onmi	☞ 1.32 PM (7 minutes ago) ☆	- + ·
	This email has an attachment to careful. Learn more	hat allows unverified scripts to run	on your computer when opened. I	Вө
	You've received an encrypted of To view your message Save and open the attachment Sign in using the following em	message from wwildcat@email.en (message.html), and follow the in ail address: wilmaathome@gmail.	zona.edu structions. com	
	This email message and its attachme confidential information. If you have	ints are for the sole use of the intended received this email in error, please not	recipient or recipients and may contain ly the sender and delete this message.	
	A Message encryption by Mi	crosoft Office 365		
	😫 message.html			
ze is enc	rvnted			

# **Encrypting Drives**

Windows 10 & Mac OS X



### TPM – Trusted Platform Module

A computer chip that is part of the computer motherboard, the TPM provides hardware-based, security related functions such as carrying out cryptographic operations.

To make use of BitLocker, your device must have a TPM.



### **BitLocker & Windows Version**

The Home version of Windows installed on *most* consumer grade computers cannot use BitLocker.

If you have a TPM and the Home version of Windows, there are other methods of encrypting your hard drive.



# Checking if your Computer has a TPM

#### STEPS

- Press "Windows Key + R".
- Type "tpm.msc" in the open text field and press enter.
- If you do not have a TPM, you will see *"Compatible TPM cannot be found".*
- If you have a TPM you will see the window on the right.

<ul> <li>Trusted Platform Module (TPM) Management on Local Computer</li> <li>File Action View Window Help</li> <li>File I</li> </ul>	- D × _ &
Search Comp TPM Management on Local Comp TPM Management on Local Computer	Actions
TPM Management on Local Comp         TPM Management on Local Computer Configures the TPM and its support by the Windows platf.           Overview         Windows computers containing a Trusted Platform Module (TPM) r features. This snap in displays information about the computer's TF administrators to manage the device.           Status         The TPM is ready for use.           Available Options         You may clear the TPM to remove ownership and reset the TPM to Manufacturer Information           Manufacturer Information         Manufacturer Version: 1.3.1.(	Actions         TPM Management on Local Computer         Prepare the TPM         Clear TPM         View         New Window from Here         Refresh         Help
< >> < >>	

#### Windows 10



# How to Turn on TPM

#### STEPS

- Press the "Windows Key + R" and type "tpm.msc" to open the TPM Management Console.
- In the Action pane, click "Turn TPM On" or "Prepare the TPM", to open a new window. Please read the message that appears.
- Shutdown or restart your computer and follow the prompts.

Trusted Platform Module (TPM) M	lanagement on Local Computer	- 🗆 ×
File Action View Window	Help	_ <i>B</i> ×
🐜 TPM Management on Local Comp	TPM Management on Local Computer	Actions
Solution Temperature for the second s	TPM Management on Local Computer Configures the TPM and its support by the Windows platfor Overview         Windows computers containing a Trusted Platform Module (TPM) p features. This snap-in displays information about the computer's TP administrators to manage the device.         Status         The TPM is ready for use.         Available Options         You may clear the TPM to remove ownership and reset the TPM to Manufacturer Information         Manufacturer Information         Manufacturer Name: NTC       Manufacturer Version: 1.3.1.(	Actions         TPM Management on Local Computer         Prepare the TPM         Clear TPM         View         New Window from Here         Refresh         Help
× >	) < >	

#### Windows 10



# Encrypting Drive in Windows 10 (Not Home)

#### STEPS

- 1. Press "windows key + e" and locate the drive to encrypt.
- 2. Right click on the local disk drive to encrypt and select "Turn on Bitlocker".\*
- 3. Choose "Enter a Password".
- 4. Select "How to Enable a Recovery Key" and follow prompts.
- 5. Choose "Encrypt Entire Drive", the most secure method.
- 6. Select "Start Encrypting" to begin.

Operating system drive

C: BitLocker on





Suspend protection 😑 Back up your recovery key Turn off BitLocker



# Encrypting Drive in Windows 10 (Home)

#### STEPS

- 1. Open the "Start Menu" and click "Settings".
- 2. Click "Updates & Security".
- 3. Click "**Device Encryption**", towards the bottom of the list on the left.
- 4. Click "Turn On".

box Box Drive

B

di sala

-##

 $\bigcirc$ 

Ο

R

**\_** 

 $\sim$ 

្រែះ

也

Calculator

Calendar

Camera





Update & Security Windows Update, recovery, backup

#### Device encryption

Device encryption helps protect your files and folders from unauthorized access in case your device is lost or stolen.

Device encryption is off.





# Encrypting Drive in Mac OS X

#### STEPS

1. Choose Apple menu and click "System **Preferences**", then click "Security & Privacy".

2. Click the "FileVault Tab".

3. Click i , then enter an administrator name and password.

4. Click Turn On "FileVault".

5. Choose how you would unlock your disk and reset your password, in case it is forgotten.

		Security 8	& Privacy		Q Search
FileVault se encrypting WARNING: Y recovery key password an	General ecures the d its contents ou will need y is automatica d recovery ke	FileVault ata on your of automatica our login pass ally generated y, the data wil	Firewall disk by lly. word or a rec as part of thi be lost.	Privacy Turn C overy key to acce s setup. If you for	Dn FileVault ss your data. A get both your
Filevault is	turned on 1	or the disk "	Macintosn	н <b>D</b> .	



Click the lock to prevent further changes.





# Encrypting Documents & Folders

Windows 10 & Mac OS X



# You Should Know!

#### **Best Practices**

- Encrypt your entire disk drive.
- Use e-mail encryption. Send encrypted TEST messages before emailing restricted data.
- Encrypting single files or folders is not a replacement for encrypting your entire disk drive or using e-mail encryption.





# **Encrypting Documents in Microsoft Office Suite**

Word, Excel, PowerPoint, etc.

#### STEPS

- Open the document.
- Click "File" in the top left of the window.
- Click on "Info".
- Select "Protect [Document]".
- Click "Encrypt with Password" and enter password.
- Use encrypted email to send encrypted document as an attachment. Provide password separately.

Encrypt a document or folder.docx - Read-Only - Saved to this PC

Mora

#### Info

#### Encrypt a document or folder

original file.

E-mail attachment: C:\Users\jamesmorales\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\Wi

F

#### Read-Only Document This file has been opened in read-only mode. Changes cannot be made to the

Save As

Save As

 $\bigcirc$ 

斺 Home

🗋 New

🗁 Open

Info

Save

Save as Adobe

Share

Export

Transform

Close



#### Protect Document

Control what types of changes people can make to this document.



#### Inspect Document

Before publishing this file, be aware that it contains:

- Document properties and author's name
- Headers
- Content that people with disabilities are unable to read



#### Version History

View and restore previous versions.



#### Manage Document

There are no unsaved changes.



# Encrypting PDFs in Adobe

#### Acrobat DC

#### STEPS

- Open PDF with Adobe Acrobat DC.
- Navigate to "**Tools**" at the top of the window.
- Scroll down and click "Protect" under "Protect & Standardize".
- A new toolbar at the top of the document offers a variety of options.
- Click "Protect Using Password", select the options and enter a new password.

Pi	rotect & Standar	rdize				
	Protect Open -	Redact Add 💌	PDF Standards	Optimize PDF	Print Production	
Home To	Accessibility Add - Dols HPP-SEC-10	00 HIPA ×				
B ☆ Protect	ቀ 🖶 🔍	①    ④    ▲ / 4     □	4 🔖 🖑 $igodot$ sect Using Password 🔀	⊕ <u>123%</u> ▼	🐨 🔛 🖉 🖾 🏷	
	Protect Using Pa	assword				
	Requires user to enter Viewing Editing Type Password Re-type Password	r a password for:				
	Advanced Options ~	Cance	Apply	<b>⊼</b> T⊦	IE UNIVERSITY	

# **Encrypting Folders in Microsoft Windows 10**

#### STEPS

- Navigate to the location of the folder and right click on the folder that you want to encrypt.
- Select "Advanced".
- Check the box "Encrypt contents to secure data".
- Click "OK".



#### Advanced Attributes

 $\times$ 

	Choose the settings you want for this folder.
	asked if you want the changes to affect all subfolders and files as well.
	Archive and Index attributes
	Eolder is ready for archiving
$\times$	Allow flag is this folder to be a sector to independ in addition to flag
sions Customize	properties
Security	
	Compress or Encrypt attributes
	Comprose contante to save disk anaco
	Encrypt contents to secure data Details
:S	
bytes)	OK Cancel
hutae)	
bytes	
20. 2-25-05 PM	
plies to files in folder)	
Advanced	
	A THE UNIVERSIT
Cancel Apply	

# Stache

**Password Storage** 



### Stache

#### What is Stache?

A secure backup of sensitive data including encryption keys, passwords, passphrases, and personal identification numbers.

Provides views of stored, shared, and digital certificate entries.

https://stache.arizona.edu/





### Stache

#### Steps for using Stache

- 1. Go to https://stache.arizona.edu.
- 2. Log in with your **UA NetID** and **password**.
- 3. Select new entry.
- 4. In the **nickname** field, enter a name that will remind you of the information you are storing. This field is not encrypted, so do not put any sensitive information (such as your password) here.
- 5. The next three fields (purpose, secret, and memo) are all encrypted, so you can put sensitive data in them. The lock icon next to these fields indicates that their contents will be encrypted. You do not have to use all three fields.
- 6. Enter any username and password information and any login details that you want to store.
- 7. If you want to share a password with another faculty or staff member (you should never do this with your UA NetID password), enter their NetID in the **Share with...** field.
- 8. You can use the **add tags** field if you want to later search by category although this is not necessary. This field is not encrypted.
- 9. Save the entry.
- 10. You will be redirected to your main Stache site, where you can see all of your entries. Entries that you have created are blue, while entries that have been shared with you are green.



# UA Box Health



### UA Box Health

#### Information

- HIPAA compliant secure cloud storage solution.
- Requires training prior to use (HIPAA Privacy Program).
- Box Health training program includes instructions on how to use Box Health.



Menu

 UA BOX Health Training Module-T.
 UA BOX Health Navigation Instructions

About UA Box Health Learning Objectives What is UA Box Health UA BOX Health Storage Guidance About UA Box Health Remember Understanding Folder Ownership UA Box Health Naming Conven.. Official Box Apps Box Tools Box Sync Collaborators & Sharing Training and Certification UA Box Health Audits Summary UA BOX Health Training Compl... Questions?





# Other resources/references

#### Resources

- ISO <u>Encryption Guideline</u>
- **Classification Standard**
- https://it.arizona.edu/documentation/uaconnect365-email-encryption
- https://it.arizona.edu/documentation/email-encryption





# Thank you for helping to keep our restricted data secure!

