



THE UNIVERSITY OF
CHICAGO
MEDICINE &
BIOLOGICAL
SCIENCES

Email and Device Encryption

UCM and BSD Information Security Offices

Agenda

- What is encryption?
- Why is encryption important?
- Who needs to use encrypted devices?
- What devices need to be encrypted?
- How do I know if my devices are encrypted?
- Email Encryption
- Q&A



What is encryption?

- Encryption helps protect your data by “scrambling” it so that it becomes unreadable.
- Only someone with the right encryption key (which is like a very long password) can decrypt and read the data.
- Full disk encryption encrypts the entire device, including all data in your files and stored in applications.
- Email encryption allows you to send emails through a secure portal.
- Email encryption protects the emails and any attachments because they reside in the secure portal rather than in plain view in an email inbox.
- Even if your email account was hacked, the encrypted messages and attachments could not be read by the hacker.

PASSWORD PROTECTED \neq ALWAYS ENCRYPTED*



Encryption Example

Text to Encrypt or Decrypted Text

This is regular text. When it is encrypted it cannot be read without the password that was used to encrypt it. You can copy and paste information here from other programs and encrypt it. For example, if you wanted to encrypt an email message you could copy the email contents here, encrypt it, paste it back into your email program, and then send an encrypted message.

Text to Decrypt or Encrypted Text

```
5A6DC3542CA6C7910CC2F22C65EC2C4244910D0C42442B2F930B87F024575C2DE062D581
E0134D152C198A709289E34FE9C3898861D3ED25F76E7B08381FD26C3EEA7341B0297B2D
F92EA1D253C65CA0C5DF2D61F64EBD96A880233045D8D70731AEC1F3189CD5BCF2E4E5F
7B9549C7CB42BD0CC74E2338C02E85E250F0A5DB39D0BE3DC93849B3142BA64407020806
3B6B8324FA3305FB11D74A2C048C10B9CAA85D960010CB68B6AA9CF5DF9F1BEA78802D6F
B16BE4C21AEB84A90A6638712D27DB5C3FD1392840280084B13FEAA1AA84D4AE189650BE
18A882E971399C63AB208B8AF74F7B0EC1D41EA2C21345B3F4D8AE746D779ADFE7D71478
22EAA1B66C55582A4C171F89B4242F3BFBF656B20D72902AC321E5E71C08FE848B3B76312
207DE7C2EA42FB24875B34093F4E1FC5F0CD1C30C590CAEDDAC3F3C462A7351E21D77780
```



Why is encryption important?

- Protects data if your device is ever lost or stolen:
 - Passwords
 - Documents and files
 - Any personal information stored
- Given we are a Healthcare system, if a device is lost or stolen the organization must be able to prove encryption was in place to enable Safe Harbor. Otherwise...
- Exhaustive and costly processes, which can take up to 100 hours, must be instantiated to determine exposures of Restricted Information. Such as:
 - An interview with the device holder by Legal, Compliance and Security
 - Forensic evaluations and use of outside counsel
 - Engaging with senior leadership of the department
 - Exhaustive further education and training, and much more

According to a report from Kensington:

- 1 laptop is stolen every 53 seconds
- 70 million smartphones are lost each year (only 7% are recovered)



Who needs to use encrypted devices?

You should be using an encrypted device if:

- You are using the device for business purposes. This includes:
 - Accessing your UCM/BSD email
 - Accessing UCM/BSD applications
 - Accessing UCM/BSD data

IF YOU ARE USING A DEVICE FOR ANY WORK-RELATED PURPOSES, IT SHOULD BE ENCRYPTED.

Consideration for Basic Sciences can be made, with exception, but even employees of these departments are exposed to health information and Social Security Numbers.

Special note: A Limited Data Set is still Protected Health Information and must still be encrypted.



What devices need to be encrypted?

ALL devices used for UCM/BSD work-related purposes need to be encrypted. This includes:

- Laptops
- Mobile phones
- Tablets
- USB/Thumb drives



Policy and Guidelines for Encryption

PREFERENCES, LEAST AMOUNT OF EFFORT

1. If you are a UCM department, your device must be procured, provisioned, managed and supported by CBIS.
2. If you are a BSD department supported by CBIS, procure and use a device provisioned and supported by CBIS.
 - Such devices come with encryption enabled and are tracked for you
3. If you are supported by a BSD IT department, procure and use a device provisioned and supported by that BSD IT department
 - These devices are also encrypted and tracked for you

ALTERNATIVES, MOST AMOUNT OF EFFORT

BSD Encryption Self-Service and Registration: <http://security.bsd.uchicago.edu/leap/>


4. Leverage the BSD Self-Service Offerings within the link above to enroll your Apple or Windows devices into the automated encryption management system.
5. You may encrypt your device following the recommendations of the BSD and UCM Information Security Offices. Evidence of the encryption must be registered using the link above.




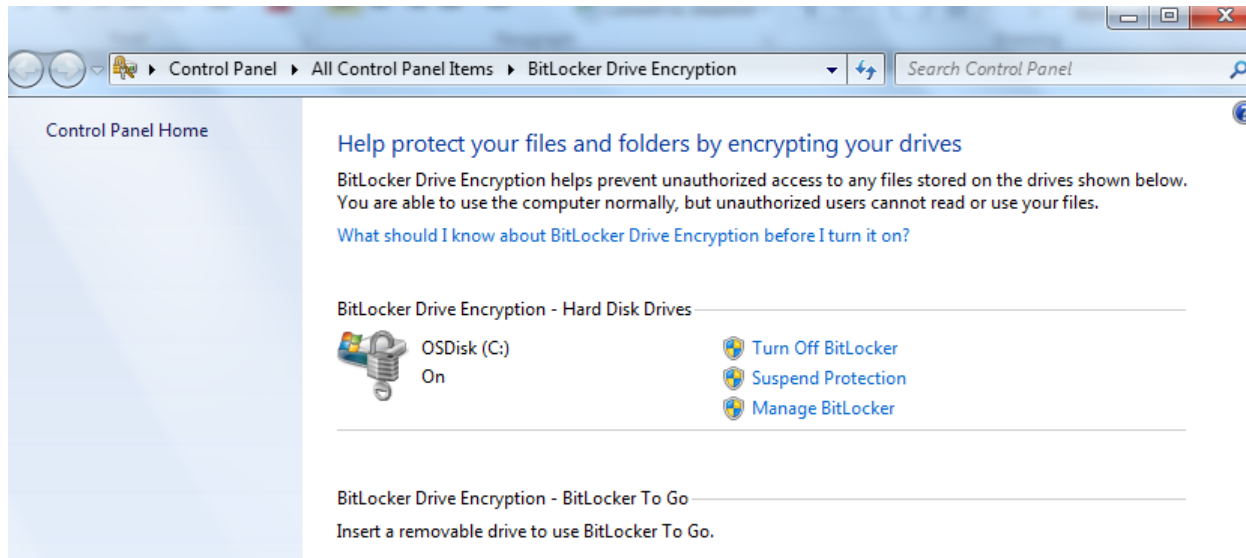
How do I know if my devices are encrypted?

Windows:

Windows devices are encrypted using BitLocker.

- Click on the Start button 
- Type “bitlocker” in the search box
- The BitLocker status will display.

 See more results



How do I know if my devices are encrypted?




- If it displays “OSDisk (C:) On” then your device is encrypted.
- If not, then you can click on “Turn on BitLocker” to encrypt your device.

Note: If you are encrypting your device without IT support, then you must create a copy of the encryption key before the encryption occurs. You can do this with a thumb drive or a local share on the file system.

How do I know if my devices are encrypted?

Macs:

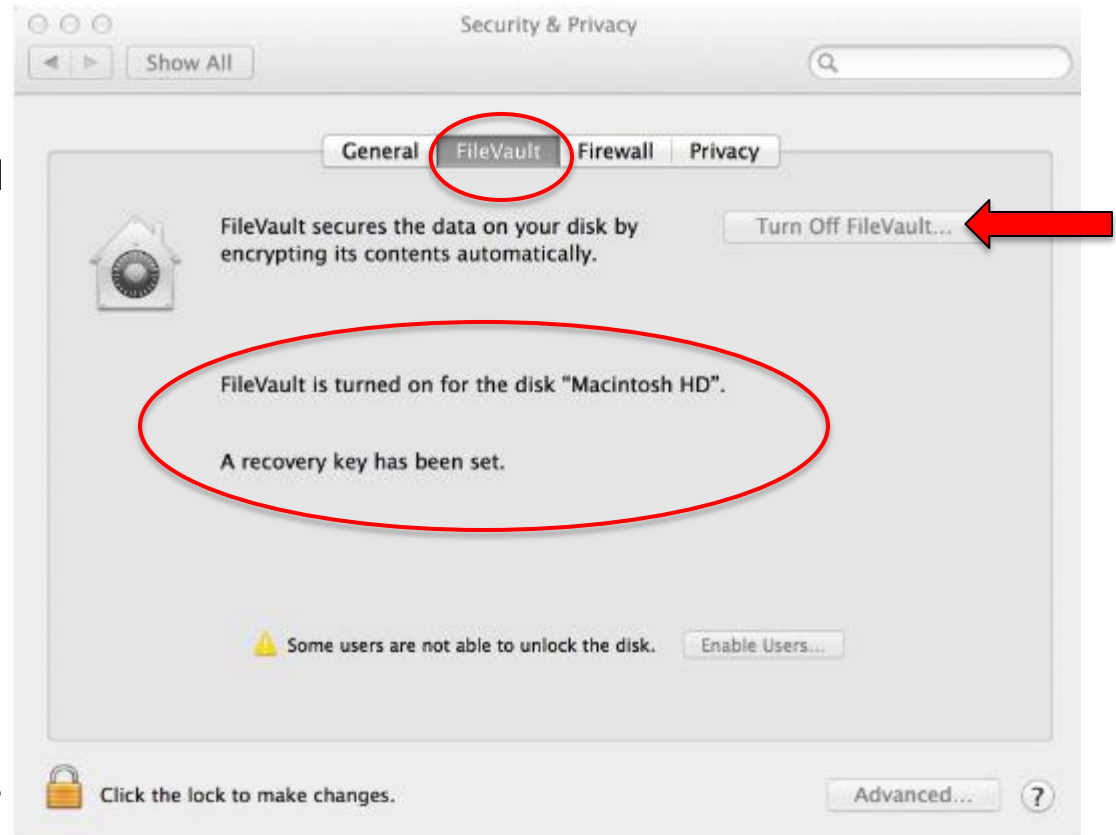
Apple (Macintosh) devices are encrypted using FileVault 2.

- Click on the Apple button  in the upper left hand part of your screen.
- Select “System Preferences.”
- Click on “Security & Privacy.”



How do I know if my devices are encrypted?

- Click on the “FileVault” tab.
- If your device is encrypted, it will state that FileVault is turned on and that a recovery key has been set.
- If it is not turned on, you can click “Turn on FileVault.”



Note: If you are encrypting your device without IT support, then you must create a copy of the encryption key before the encryption occurs. You can do this with a thumb drive or a local share on the file system.

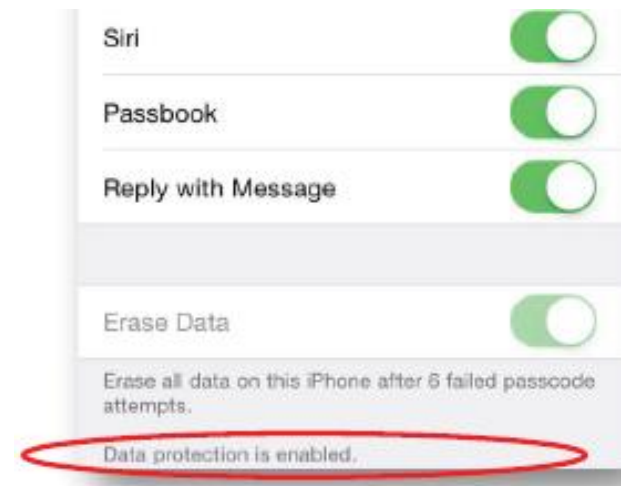
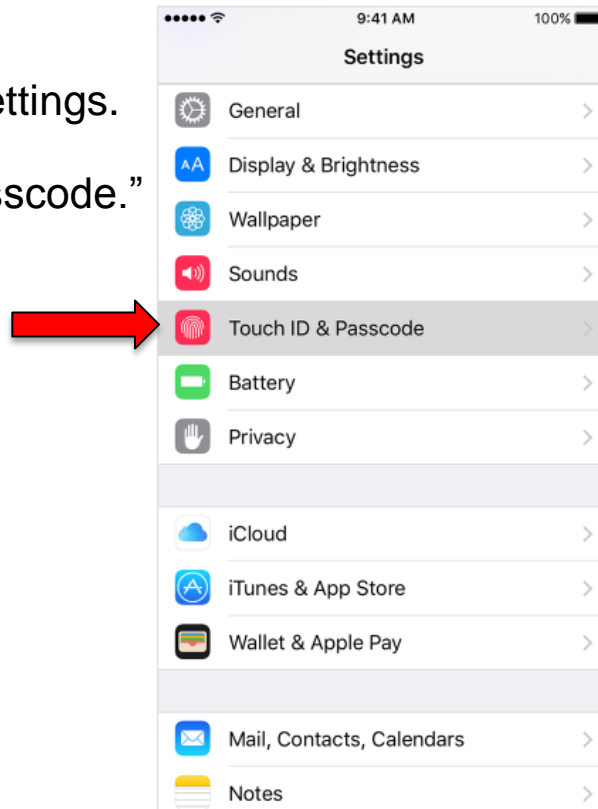


How do I know if my devices are encrypted?

Apple Mobile Devices:

Starting with iPhone 3, iPad 1, and iPod Touch 3, the device is encrypted as long as the passcode is enabled.

- On your device, go to Settings.
- Select “(Touch ID &) Passcode.”



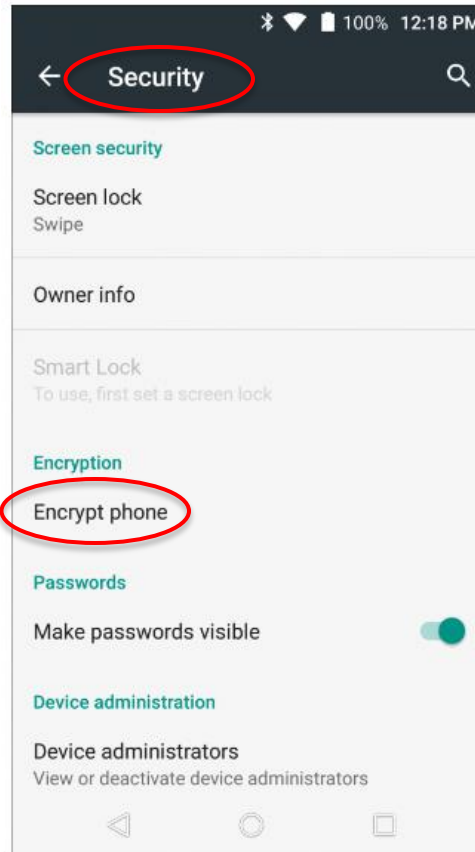
How do I know if my devices are encrypted?

Android Mobile Devices:

Unlike with Apple devices, Androids do not automatically encrypt the device when the passcode is enabled.

- Make sure your device has a passcode enabled.
- Go to the “Settings” screen.
- Click on “Security.”
- Select “Encrypt phone” or “Encrypt tablet.”

Note: Before encrypting your device, make sure you have a backup of your data. Also pay attention to the warnings that are displayed.



How do I know if my devices are encrypted?

Thumb drives:

UCM

- Encrypted thumb drives are available for purchase through the UCM Supply Chain (Staples Advantage Catalog).
- The Kingston Data Traveler 4000 series (formerly IronKey) is approved for use.

BSD

- Encrypted thumb drives are available for purchase through Buysite at Staples.
- The Kingston Data Traveler (formerly IronKey) and Apricorn Aegis are approved for use.



Kingston® DataTraveler® 4000 G2 8GB USB Flash Drive, Black

Staples Item # 1621244

MFR Item #DT4000G28GB

★★★★★ (Not yet rated)

Compare



Device Encryption Resources

BSD Information Security Office Website:

- Encryption: <http://security.bsd.uchicago.edu/encryption>
 - Laptop Encryption: <http://security.bsd.uchicago.edu/leap/>
 - Mobile Device Encryption: <http://security.bsd.uchicago.edu/bsd-mobile-device-encryption/>
 - USB Encryption: <http://security.bsd.uchicago.edu/bsd-usb-encryption/>
 - Laptop Encryption Certification: <https://redcap.uchicago.edu/surveys/?s=frPnX2cPHE>
This form provides an attestation that your laptop is encrypted.

UCM Information Security Office Intranet Webpage:

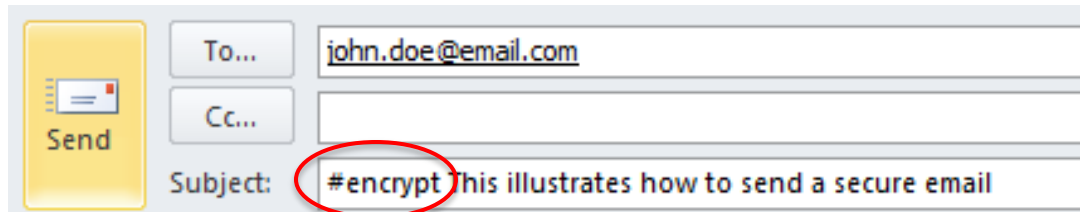
- Encryption Tip Sheet: <http://home.uchospitals.edu/> Go to Quick Links on the left hand side of the screen and click on “Information Security Office” > Encryption Tip Sheet



Email Encryption

The Secure E-Mail Portal provides a secure way for employees to email Restricted information, such as PHI, to recipients outside of UCM and the BSD.

- Ensure that emails are sent on a need-to-know basis for business purposes.
- Type **#encrypt** in the subject line of the email.



The screenshot shows an email composition interface. On the left is a yellow 'Send' button with an envelope icon. To its right are three input fields: 'To...' containing 'john.doe@email.com', 'Cc...' which is empty, and 'Subject:' containing '#encrypt This illustrates how to send a secure email'. The text '#encrypt' in the subject line is circled in red.

- The subject line is not encrypted; only the body of the email and attachments are encrypted.

Email Encryption

- When the email recipient receives the secure email, they will get a message requesting that they click on the link to view the email.



- They will then be asked to create a password which will be used to view the email and any subsequent emails from UCM/BSD.

Email Encryption Resources

BSD Information Security Office Website:

- <http://security.bsd.uchicago.edu/bsd-e-mail-encryption/>

UCM Information Security Office Intranet Webpage:

- Data Guardian Program: <http://home.uchospitals.edu/> Go to Quick Links on the left hand side of the screen and click on “Information Security Office” > Data Guardian Program



Contact Us

Department	Email
UCM Information Security Office	security@uchospitals.edu
BSD Information Security Office	security@bsd.uchicago.edu

