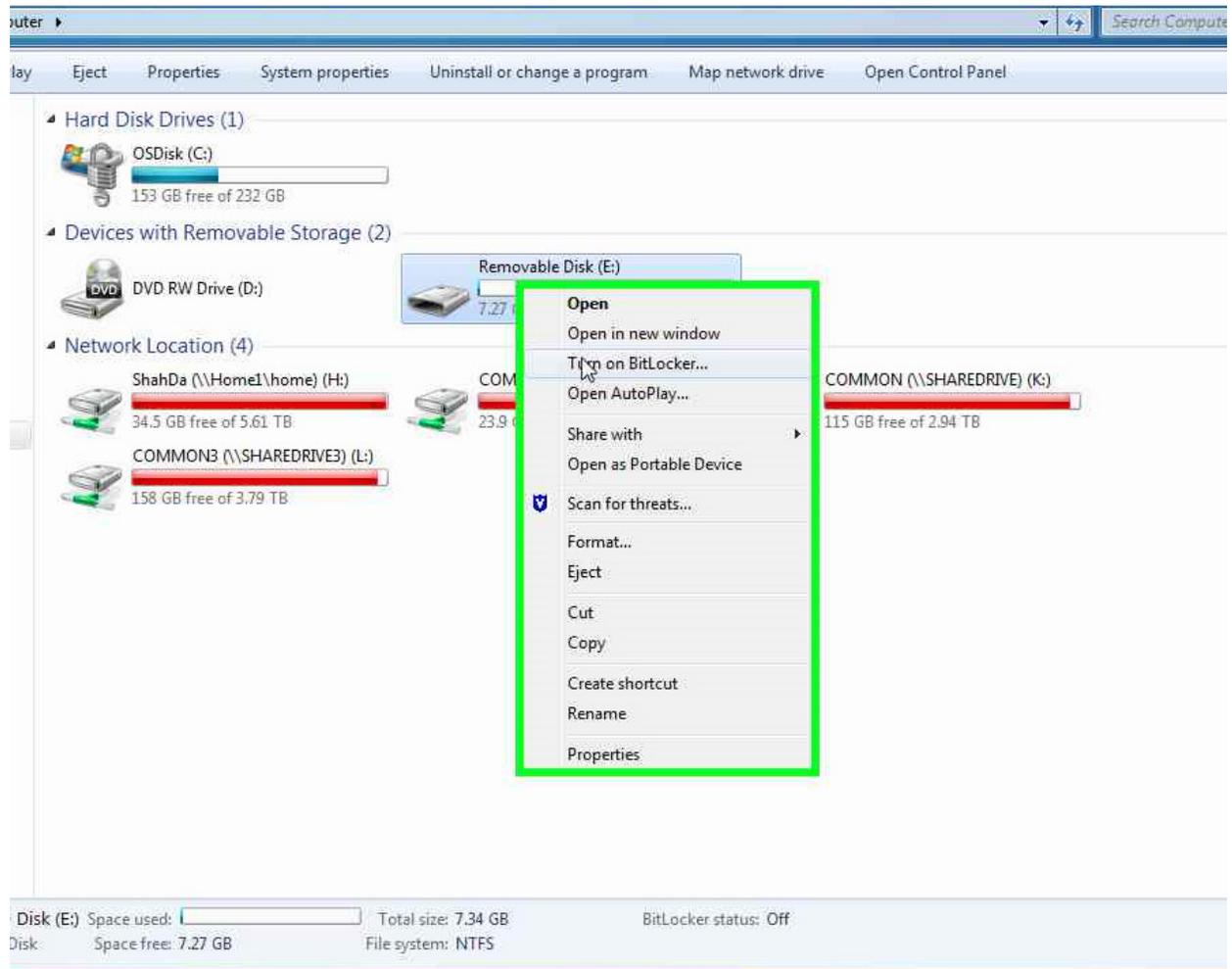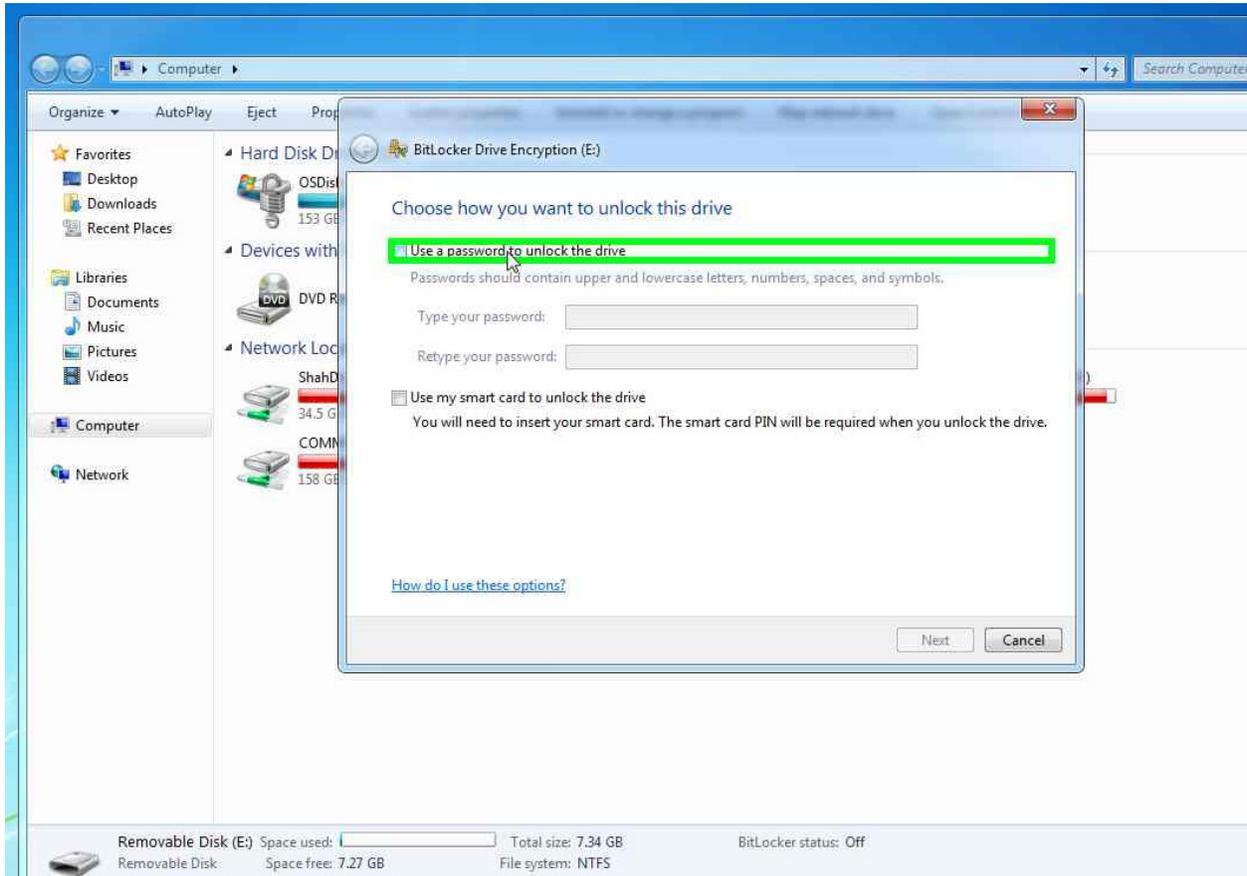# Encryption of Removable Drive Using BitLocker on SMHPC Computers

Step1: Right click on the Removable disk (USB Drive) and select " Turn on BitLocker… "

Step2: Select "Use a password to unlock the drive", enter a strong* password and click next.

*Note: A "strong password" is defined as per SMH Information Security Policy, Password Management:

5.1. Password Strength

A Strong Password is a password that is long enough and complex enough that it is very difficult to defeat, even by automated means. SMH systems must ensure that user accounts that provide access to critical systems—such as major clinical systems--have strong passwords. When possible, Users should use phrases (e.g., IL0v3EatingP!zza).

Accordingly, passwords for critical systems must have a minimum length of eight (8) characters and the following three additional characteristics:

- at least one uppercase character
- at least one lowercase character
- at least one numeric character

The optional use of non-alphanumeric characters (~!@#$%^&*_-+=' |\(){}[]:;"'<>,.?/) may further increase the strength of a password.

Users must never create passwords that include:

- All or part of the User ID
- Easily obtained personal information about themselves (e.g., name of family members, pets, birthdays, anniversaries, hobbies, etc.)
- Three identical or consecutive characters (e.g., AAA, 123, abc)

.

Step 3: Print recovery key for recovery purposes and store it securely. Alternatively, you can select save recovery key to a file and save it on your H drive.
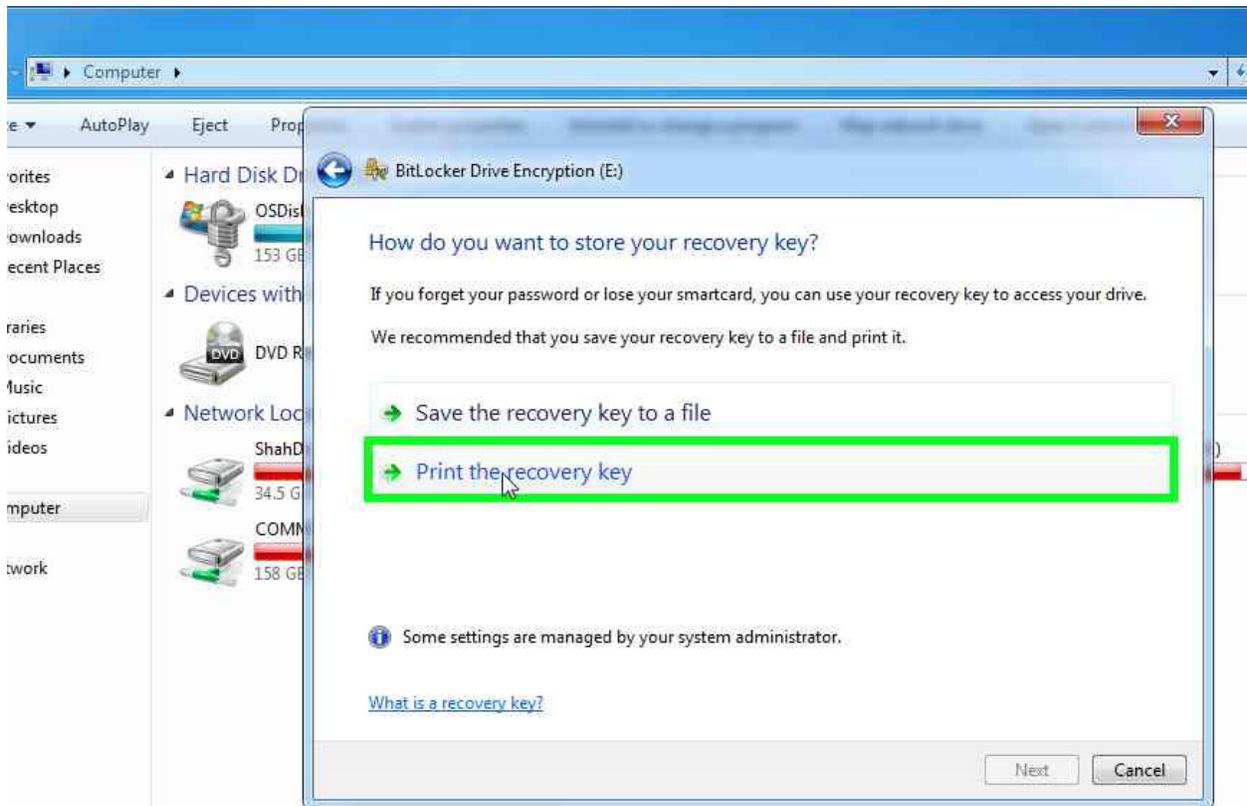
Step4: Click "start encrypting" to start the encryption process. Depending on the size of USB it may take from a few minutes up to one hour to complete the encryption process. Once completed, the USB drive can be used as usual.

How to access an encrypted drive?

Step 1: Inserting an encrypted drive will provide you with a prompt asking for credentials.

Step 2: Enter the password and click unlock.

You can now use the drive as you would normally use it.

(ds/July 4th, 2016)