Secure your research data using encryption

LONDON SCHOOL of HYGIENE &TROPICAL MEDICINE

Encryption is a method by which data – digital or otherwise – is converted into a scrambled form that can only be decoded and read if the user possesses an appropriate key. It serves as a method for protecting information from unauthorised access.

Research data to be encrypted

Encryption should be applied to several types of research data:

- Personally-identifiable information that describes study participants and other individuals
- Commercially sensitive information that has been provided by a third party;
- Other sensitive information that requires protection

Types of data encryption

Data that requires protection must be encrypted for the entire period it is held. This includes:

- Data at Rest: Data held on mobile devices, desktops/laptops and storage media should be protected to prevent unauthorised access.
- Data in Motion: Data to be transferred from location A to B should be encrypted to prevent it being intercepted and accessed. This covers electronic transfer (e-mail, FTP, etc.) and physical transmission (e.g. sending a USB disk through the post).

Encryption is only effective when a third party does not have access to the encryption key. If a user has entered the password for an encrypted drive and left their machine unattended or provided the password in the same email as the encrypted file, the data will not be secure.

Research data can be encrypted at several levels:

- Disk encryption: The content of a drive or specific partition are encrypted. Common tools include BitLocker for Microsoft Windows and FileVault for MacOS.
- Encrypted container: A file that, when accessed using appropriate software, can be accessed and used in the same way as a physical drive. Vera Crypt, a derivative of True Crypt, is often used for this purpose.
- Encrypted archive: Compression software, such as 7zip, may be used to create an archive that can be accessed only by entering the correct encryption password.

Encryption security levels

A simple rule to compare the security of different encryption algorithms is to look at the key size – a key with a large number (256 bits) is more secure than one with a smaller number (128 bits).
For health data, an encryption algorithm with a key length of 256 bits should be used, such as AES 256, 3DES, or Blowfish, as recommended by NHS Information Governance Guidelines.

Book an appointment

To discuss your data security arrangements, contact the LSHTM Research Data Management Service at researchdatamanagement@lshtm.ac.uk.

Further information:

- LSHTM: Encrypting data using VeraCrypt - http://researchonline.lshtm.ac.uk/3716462/
- LSHTM: Encrypting data using 7-Zip - http://researchonline.lshtm.ac.uk/3716462/
- LSHTM: Encrypt iOS/Android - https://www.lshtm.ac.uk/aboutus/organisation/information-management-and-security
- UK Data Service: Encrypt files using VeraCrypt [video] - https://www.youtube.com/watch?v=Ogm9QHQpFqU
- UK Data Service: Encrypt files using FileVault [video] - https://www.youtube.com/watch?v=JIZ9EFMS0ic
- MANTRA Online Learning Unit – Storage and Security - http://datalib.edina.ac.uk/mantra/

https://doi.org/10.17037/DATA.50. Reviewed: July 17 2017