Staines Road Surgery

Exchange of Information

Introduction

This standard is in place to prevent loss, modification or misuse of information exchanges between organisations.

Risk Management

The risks identified under this policy include unauthorised access to information, misuse of information, loss of information, unauthorised disclosure of information, breach of legislation.

1.0 Information Exchange Agreements

1.1 Agreements will be established for the exchange of information and software (whether electronic or manual) between organisations and will consider:

- management responsibilities for controlling and notifying transmission, despatch and receipt
- procedures for notifying sender, transmission, despatch and receipt
- minimum technical standards for packaging and transmission
- courier identification standards
- responsibilities and liabilities in the event of loss of data
- use of an agreed labeling system for sensitive or critical information, ensuring that the meaning of the labels is immediately understood and that the information is appropriately protected
- information and software ownership and responsibilities for data protection, software copyright compliance etc
- technical standards for recording and reading information and software
- any special controls that may be required to protect sensitive items, such as cryptographic keys.

2.0 Security of Media in Transit

2.1 The following controls will be applied to safeguard computer media being transported between sites.

- reliable transport or couriers will be used. A list of authorised couriers will be agreed and procedures to check the identification of couriers will be implemented
- adequate packaging will be used to protect the contents from any physical damage likely to arise during transit and will be in accordance with manufacturers' specifications.
- additional controls will be applied where necessary to protect sensitive information from unauthorised disclosure or modification, for example:
    - use of locked containers
    - delivery by hand
    - tamper-evident packaging
    - use of digital signatures and encryption

3.0 Security of Electronic Office Systems

3.1 Guidelines will be developed and implemented to control the business and security risks associated with electronic office systems.

4.0 Publicly Available Systems

4.1 A formal process will be implemented to ensure that information is authorised before being made publicly available and the integrity of such information will be protected to prevent unauthorised modification.

5.0 Other Forms of Information Exchange (e.g. faxes, mobile phones)

5.1 Procedures will be implemented to protect the exchange of information through the use of voice, facsimile and video communications facilities and should include:

- Staff will be reminded that they should take appropriate precautions, e.g. not to reveal confidential / sensitive information such as to avoid being overheard or intercepted when making a phone call
- Staff will be reminded that they should not have confidential conversations in public places or open offices and meeting places with thin walls.
- Not leaving messages on answering machines
- Not writing confidential / sensitive information on white boards

5.2 Guidelines will be developed and implemented for the use of facsimile.