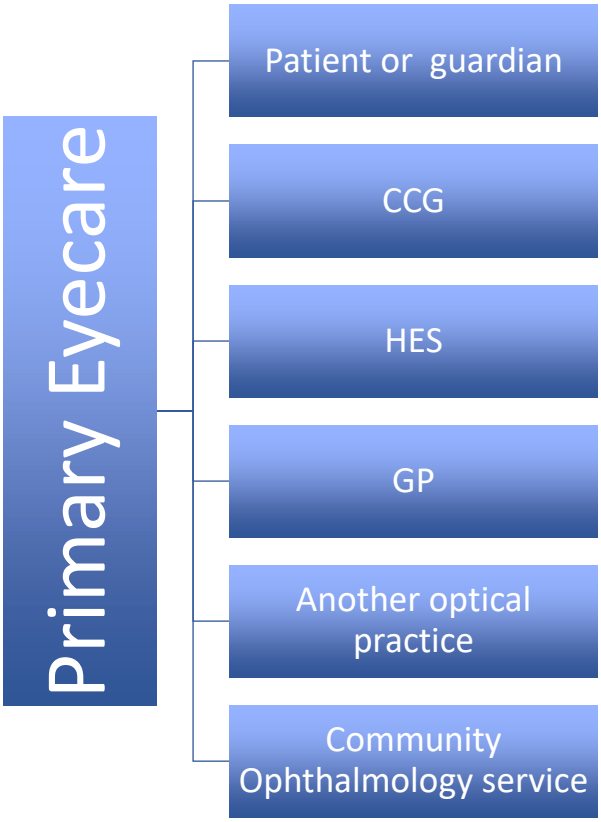
Document name:	*[ ]: Information security assurance – data transfer*
Date created:	*13 March 2017*
Author:	*Jane Smellie*
Approved by:	

Requirement 322: Data Flow and Transfer

This document outlines the procedures that should be followed where sensitive or person identifiable information is being transferred to or from the company. These procedures are in place to help prevent unauthorised access to information, loss of information, unauthorised disclosure of information or breach of legislation.



Describe the nature of the information flow between the Company and the external organisation, e.g. data item, format, transfer method	Identify the type and risk level of breaches of confidentiality	Describe the measures taken to mitigate the risk of breaches in confidentiality of information that is passed between the company and the external organisation
Patient or Guardian		
Referral letter copies, patient recall letters	Low	Information only sent to confirmed patient address by post.
CCG		
Performance reports as per the th Specification for community services	Low	Data is anonymised and sent by NHS mail.
HES		
Referral letters	Low	Sent by post, fax to safe Haven, or email using NHS Mail.
GP		
Referral letters or feedback reports on patients who have been referred to the community service	Low	Sent by post, fax to safe Haven, or email using NHS Mail.
Another optical practice		
Feedback reports on patients who have been referred to the community service	Low	Sent by post or email using NHS Mail.
Community Ophthalmology Service (if applicable)		
Referral letters	Low	Sent by post, fax to safe Haven, or email using NHS Mail.

1. Maintaining Confidentiality of Data Received (Safe Havens)

The term safe haven is a term used to explain either a secure physical location or the agreed set of administrative arrangements that are in place within the company to ensure confidential personal information is communicated safely and securely.

The company's 'safe-haven' is the location for patient information to be securely received.

A. When paper-based information is received it will be stored securely, as soon as practical.

B. Computers should not be located where their usage can be observed to avoid unauthorised access.

i. Passwords are kept confidential and not written down or shared.
ii. Password protected screensavers will be used where possible.
iii. Laptop computers will be locked up when not in use.

C. Confidential conversations will be held where they cannot be overhead by members of the public.

2. Only Transferring Data where Appropriate

A. The personal information contained in transfers will be limited to those details necessary in order for the recipient to carry out their role.

B. Before transferring data, it will be considered whether there are any patient consent requirements that must be met before the transfer is made:

A. A record of consent should be maintained where required.
B. Patients will be given the right to choose whether or not to agree to the use or disclosure of their personal information and the patient has the right to change their decision about a disclosure before it is made.
C. Only persons authorised by the Company will have responsibility for obtaining consent for non-healthcare purposes, for example research.
D. If the patient has detailed questions about consent, they will be referred to the Clinical Governance and Performance Lead.
E. If circumstances change, relevant to the sharing of consent, for example if there is a change of recipient, consent will be reaffirmed.

3. Securely Transferring Data

Consideration needs to be given to the mode of transfer and whether any specific controls are required to maintain the confidentiality of the data e.g. encryption on electronic transfers.

A. Verbal Communication

- Confidential messages will not be left on answer-phones (e.g. information about the patient's eye health). It might not be heard only by the intended recipient.
- Care will be taken when taking messages off answer-phones to ensure that the messages cannot be overheard inappropriately when being played back.
- When receiving calls requesting personal information the caller's identity will be verified and the reason for the request will be considered to establish whether the information can be disclosed.
- Where information is transferred by phone, or face to face, care will be taken to ensure that personal details are not overheard by other people.

B. Post

- Envelopes will be marked "Private & Confidential"
- The full postal address of the recipient will be double checked,

- The method for sending confidential information will be considered carefully based on risk of loss.
- When necessary, the recipient will be asked to confirm receipt.

C. Faxing

- If faxing personal or confidential information: a) the fax number will be double checked b) the fax header will be marked “Private & Confidential” c) a named person who needs to receive the fax will be identified.
- Faxes will not be sent to an organisation outside of their working hours where there is no-one present to receive.

D. Communication by email

- Transfer of personal information by email will be avoided other than where both sender and recipient are using an NHSmail account (nhs.net to nhs.net accounts) or the information is sent as an encrypted attachment
- If identifiable information must be sent other than via NHSmail, it MUST be encrypted to NHS standards
- The email header will make it clear that the information contains confidential information