Document name:	*Primary Eyecare Cheshire: Information Governance Policy*
Date created:	*13 March 2017*
Author:	*Jane Smellie*
Approved by:	

Requirement 115: Information Governance Policy

Purpose of the Policy

This policy sets out the procedures and management accountability and structures that have been put in place within the Company to safeguard the movement of personal data in the Company. This policy describes the data that we hold about patients, how we hold it, how we protect it, how we use and process it (including what patients need to be provided with) and how we transfer it (if necessary).

The Company has been established to specifically act as the lead for a network of local optical practices dedicated to delivering excellent eye care in the local community. Appropriate management of data is fundamental for the Company and our subcontractors.

The Company is committed to meeting the requirements of Level 2 of the NHS Information Governance Toolkit.

Webstar Health

The Company utilises Webstar Health to provide the secure online OptoManager IT platform to collect data from the service and to manage billing and payment disbursement. Webstar Health meets the requirements of Level 2 of the NHS Information Governance Toolkit.

The Company and Webstar Health have developed a joint Business Continuity and Disaster Recovery Plan.

Optical Practice Subcontractors

The Company will collect evidence from all of its subcontractor practices confirming that an information governance audit has been completed and that the all of the required policies and procedures that relate to data management and information governance are in place.

The Company requires all subcontractor practices to specifically have in place:

- Named information governance lead
- Information Governance Policy

- Confidentiality clause within the contracts of all staff
- Staff training on information governance
- Evidence of compliance with DPA where data is processed outside the UK
- Procedures for seeking consent to use patient information
- Publicly available information leaflet
- Confidentiality Code of Conduct
- Information Asset Register
- Risk assessment (including working towards implementing any high priority security improvements identified)
- Mobile computing guidelines including encryption of mobile devices storing personal data (if applicable)
- Business continuity plan
- Incident management and reporting process
- Access control and password management procedures
- Data handling procedures

The Company reserves the right to inspect subcontractors' premises and/or policies to audit compliance.

Legislative Requirements

There are certain legislative requirements for every organisation to hold information. Information about this is provided below:

- The Company complies with the eight data protection principles under the Data Protection Act 1998 in its processing of personal data in that such data is:
    - fairly and lawfully processed
    - processed for limited purposes
    - adequate, relevant and not excessive
    - accurate and up to date
    - not kept for longer than is necessary
    - processed in line with patients' rights
    - secure
    - not transferred to other countries without adequate protection
- The Company's clinical governance and performance lead is the named information governance lead trained in and responsible for procedures relating to confidentiality and data management.
- The Company is registered with the information commissioner:

    - Registration No. [ICO]
- The Company has an up to date Freedom of Information Act Statement and this is available to patients.
- A notice on handling patient data is available to patients on the Company's website.

What information the Company holds and how it holds it

- The Company holds patients' clinical records electronically within the secure online OptoManager IT platform.

How the Company protects this information

- All directors have a confidentiality clause within their contracts.
- All personal information contained on clinical records is considered confidential.
- The Company's directors are aware of the importance of ensuring and maintaining the confidentiality of patients' personal data and that such data must be processed and stored in a secure manner.
- The Company has an IT security policy regarding specific access to electronic information
- Any suspected breaches of security or loss of information are reported immediately and are dealt with appropriately by the person responsibility for confidentiality and data management.

How the Company uses and processes this information

- The Company may use the information to audit clinical outcomes and our performance. This enables it to monitor and improve the quality of care that it offers.
- Wherever possible (i.e. if the Company does not need to know who an individual patient is) it will only analyse trends from anonymised information.
- The Company's clinical governance and performance lead may need to access individual patient information if a complaint or incident requires investigation.

How the Company transfers information (if necessary)

- The commissioner will have access to anonymised information on quality and outcomes of the service.

- The Company is obliged to provide information to authorised persons within the NHS (who are in turn subject to a duty of confidentiality) if they request this. The Company always transfers data in a secure manner.

Accountability for this Policy

The designated information governance lead in the Company is responsible for overseeing day to day information governance issues; developing and maintaining policies, standards, procedures and guidance; coordinating information governance in the Company; raising awareness of information governance and ensuring that there is ongoing compliance with the policy and its supporting standards and guidelines.
The Board of Directors is responsible for ensuring that sufficient resources are available to support the implementation of information governance procedures in order to ensure compliance with legal, professional and the NHS information governance requirements.

Supporting Policies and Procedures – Directors' Responsibilities

All directors of the Company are responsible for ensuring that they remain aware of the requirements incumbent upon them and will be required to adhere to the following:

- Confidentiality Code of Conduct (sets out the standards expected of directors, staff and subcontractors in maintaining the confidentiality of patient information)
- Mobile computing guidelines and encryption of mobile devices storing personal data (provides guidance on the use of portable devices)
- Access control and password management procedures (sets out procedures for the management of access to computer-based information systems)
- Data transfer procedure (sets out procedures around the secure transfer of data, collecting consent and maintaining confidentiality within the Company including the use of safe havens)
- Business continuity procedures (sets out the procedures in the event of system failure)
- Serious Incident Policy (sets out the procedures for responding to a security breach)

Policy Review

This policy will be reviewed annually.

Sanctions

Breach of this policy could lead to disciplinary action. Depending on the circumstances this could range from remedial training to dismissal/removal from the Board.