Document name:	*Complete Ophthalmic Services CIC: Information Governance and Data Management Policy*
Date created:	*June 2015* *Review date: June 2017*
Author:	*The Directors, Complete Ophthalmic Services CIC*
Approved by:	

Complete Ophthalmic Services CIC:
Information Governance and Data Management Policy

Complete Ophthalmic Services CIC ("the Company") has been established to specifically act as the lead for a network of local optical practices ("subcontractors") dedicated to deliver excellent eye care in the local community. The Company will also utilise a non-clinical subcontractor, Webstar Health. 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.

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 will complete an organisation crime profile in accordance with NHS Protect Guidance within one month following service commencement date.The Company will subsequently take necessary action to abide by NHS Protect standards as indicated by the organisation crime profile.

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

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
- Confidentiality Code of Conduct
- Data Asset Register
- Mobile Computing Guidelines
- Encryption of mobile devices storing personal data (if applicable)
- Access control and password management procedures
- Data Handling Procedures
- Risk assessment (including working towards implementing any high priority security improvements identified)
- Incident Management and Reporting process
- Evidence of compliance with DPA where data is processed outside the UK.

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

This policy describes the data that the Company holds about patients, how itholds it, how itprotect it, how ituses and processes it (including what patients need to be provided with) and how ittransfers it (if necessary).

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 Companyis registered with the information commissioner
    - Registration No. ZA046735

- 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 (see appendix 1).

What information the Companyholds and how itholds it

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

How the Companyprotects this information

- All the Company's 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 Companyuses and processes this information

- The Company may use the information to audit clinical outcomes and our performance. This enables the Companyto monitor and improve the quality of care that itoffers.

- Wherever possible (i.e. if the Company does not need to know who an individual patient is) itwill 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 Companytransfers information (if necessary)

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

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

The Company'ssupporting policies

All directors ofthe Companywill be required to adhere to the following supporting policies:

- Mobile Computing Guidelines
- Encryption of mobile devices storing personal data (if applicable)
- Access control and password management procedures
- Serious Incident Policy.

This Information Governance and Data Management Policy will be reviewed annually with commencement date March 2014.

APPENDIX 1

Notice to be displayed on Complete Ophthalmic Services CIC website

Complete Ophthalmic Services CIC ("the Company") hold various pieces of information about you relating to community eye care services, including your name and address, and clinical details such as the state of health of your eyes, and copies of any letters we have written about you or received from other professionals, such as your doctor.You are entitled to a copy of this information although there may be an administrative charge for providing it. If you wish to see your records, please contact Charles Greenwood, Complete Ophthalmic Services CIC (020 8776 5000)and we will respond as quickly as possible. We are required to respond within 40 days. If you require independent advice, contact the Information Commissioners' Office at www.ico.gov.uk.

We adhere to the guidelines of the College of Optometrists and the Data Protection Act and will not pass any of your personal information to a third party without your consent unless there is a clear public interest duty to do so.

We are obliged to provide information to authorised persons within the NHS (who are in turn subject to a duty of confidentiality) if they request this. This is usually to confirm that we have provided the NHS services that we have been paid for, and to improve quality of care.

The Company may use the information to audit clinical outcomes and our performance. This enables us to monitor and improve the quality of care that we offer you. Wherever possible (i.e. if we do not need to know who an individual patient is) we will only analyse trends from anonymised information.

If you have any queries about this please contact us and we will be happy to help.