APPENDIX

Backup Policy

Our practice uses practice management software that is compliant with GDPR and is backed up incrementally throughout the day and then a full backup done overnight. This is encrypted and secure.

Cameron Optometry servers are monitored by an external IT consultant who provides encrypted cloud back ups daily. We also have an off site hard back up in a fire / water safe unit in the basement cellars on street level.

- We can restore quickly
- Off site backups and software discs in a fireproof safe
- Any data taken offsite should be secure (password protected or not left unattended and/or locked away)
- Online backup services encrypts the data securely before transmitting it from the practice PC
- All original software discs / downloads are safely stored.

APPENDIX

RECORD RETENTION

- This policy applies to the following:
    - Spectacle records
    - Contact lens records
    - Appointment diaries
    - Telephone and/or Tele-health consultations
- All records are retained for 10 years from the date of last seeing the patient.
- Records of children are retained until they are 25 AND it is 10 years since they were last seen.
- Records of the deceased are kept for 10 years.
- Records are destroyed by shredding.

Examples:

Age at last test	**Time to retain record**
Age 5	Until age 25
Age 10	Until age 25
Age 17	Until age 27
Over 18	For 10 years

APPENDIX

Recording of telephone calls and/or consultations

Telephone calls between patients and providers will not be recorded or monitored due to the complexity of obtaining consent for this process and the subsequent storing of patient sensitive data.

If telephone calls are to be monitored and/or recorded a specific policy will be required taking into account:

- Regulation of Investigatory Powers Act 2000 ("RIPA")
- The Telecommunications (Lawful Business Practice) (Interception pf Communications) Regulations 2000.
- The Data Protection Act 1998
- The Employment Practices, Data Protection Code.
- Human Rights Act 1998
- Code of Practice – FSA Handbook – Code of Business Handbook and Direct Marketing Association's Code of Practice, PCI DSS.
- Telecoms Licence obligations – The Service Provision Licence

Communications strategy and Implementation plan

The provider should have readily available information relating to paragraph 2(3) of Part II of Schedule 1 of the Data protection act.

(2) A data controller is not obliged to supply any information under subsection (1) unless he has received—

a. ***a request in writing, and***
b. ***(b)except in prescribed cases, such fee (not exceeding the prescribed maximum) as he may require.***

F2(3) Where a data controller—

a. ***reasonably requires further information in order to satisfy himself as to the identity of the person making a request under this section and to locate the information which that person seeks, and***

b) has informed him of that requirement, the data controller is not obliged to comply with the request unless he is supplied with that further information.]

APPENDIX

Disclosure of Data to commissioners

The practice (provider) agrees to provide anonymised, pseudonymised or aggregated data as may be requested by the co-ordinating commissioner or LOC company. Personal data will not be disclosed without written consent or lawful reason for disclosure.

Exceptions to this are covered by:

Section 251 of the NHS Act 2006 (originally enacted under Section 60 of the Health and Social Care Act 2001), allows the common-law duty of confidentiality to be set aside in specific circumstances where anonymised information is not sufficient and where patient consent is not practicable.

Data Protection Principles

Personal data must be:

1. Processed fairly and lawfully
2. Processed for specified purposes
3. Adequate, relevant and not excessive
4. Accurate and kept up to date
5. Not kept longer than necessary
6. Processed in accordance with the rights of data subjects
7. Protected by appropriate security (practical and organisational)
8. Not transferred outside the EEA without adequate protection

APPENDIX

Scottish Government Records Management: NHS Code of Practice

All data processed on behalf of the commissioner with regard to community services must be processed and handled in line with the Scottish Government Records Management: NHS Code of Practice

All staff handling data should be aware of the obligations placed upon them by the NHS Code of Practice and the commitments laid out in it.

In summary, this covers:

Why people may access patient records:

- As the basis for health decisions
- Ensure safe effective care
- Work effectively with other
- Clinical audit
- Protect health of the general public
- Monitor NHS spending
- Manage the health service
- To investigate complaints
- Teaching and research

Law relating to records

- Confidentiality under common-law duty of confidentiality
- Protection about how information is processed (Data Protection Act 1998)
- Privacy (Human Rights Act 1998)

These rights are not absolute and they need to be balanced against those of others.
Other patient rights regarding records

- To ask for a copy of all records held in paper or electronic form (a fee may be payable until 25th May 2018 – After this date no fee may be charged, unless a request is manifestly unfounded or excessive, e.g. for multiple further copies of the same information. In this case, the administrative cost of providing the information will equal the fee charged.)
- Choose someone to make decisions about the patient's healthcare if the patient becomes unable to do so (lasting power of attorney)

Duties placed upon the practice (provider)

- Maintain accurate records of the care provided
- Keep records confidential, secure, and accurate (even after the patient dies)
- Provide information in accessible formats (e.g. large print)

The Scottish Government Records Management: NHS Code of Practice
will be available for staff members to consult.

APPENDIX

Caldicott Principles

1. Justify the purpose(s) of using confidential information
2. Only use it when absolutely necessary
3. Use the minimum that is required
4. Access should be on a strict need to know basis
5. Everyone must understand his or her responsibilities
6. Understand and comply with the law

Quality Statements

1. Patients are treated with dignity, kindness, compassion, courtesy, respect, understanding and honesty.
2. Patients experience effective interactions with staff who have demonstrated competency in relevant communication skills.
3. Patients are introduced to all healthcare professionals involved in their care and are made aware of the roles and responsibilities of the members of the healthcare team.
4. Patients have opportunities to discuss their health beliefs, concerns and preferences to inform their individualised care.
5. Patients are supported by healthcare professionals to understand relevant treatment options, including benefits, risks and potential consequences.
6. Patients are actively involved in shared decision making and supported by healthcare professionals to make fully informed choices about investigations, treatment and care that reflect what is important to them.
7. Patients are made aware that they have the right to choose, accept or decline treatment and these decisions are respected and supported.
8. Patients are made aware that they can ask for a second opinion. *(This would not be funded by GOS as there is no mechanism for this)*
9. Patients experience care that is tailored to their needs and personal preferences, taking into account their circumstances, their ability to access services and their coexisting conditions.
10. Patients may have their physical and psychological needs assessed and addressed where necessary, including nutrition, hydration, pain relief, personal hygiene and anxiety.
11. Patients experience continuity of care delivered, whenever possible, by the same healthcare professional or team throughout a single episode of care.
12. Patients experience coordinated care with clear and accurate information exchange between relevant health and social care professionals.
13. Patients' preferences for sharing information with their partner, family members and/or carers are established, respected and reviewed throughout their care.
14. Patients are made aware of who to contact, how to contact them and when to make contact about their on going healthcare needs.

APPENDIX

Handling requests for Rx and clinical information

A Subject Access Request (SAR) allows individuals (including ex-patients and ex-employees) to access personal data that is held about them in any format (subject to some safeguards). You must respond to an SAR within **one month.**

- We will respond to any SAR within one month
- There will be no charge to the individual making the SAR, unless a request is manifestly unfounded or excessive, e.g. for multiple further copies of the same information. In this case, the administrative cost of providing the information will equal the fee charged.

Spectacle Prescription (Spec Rx) or Contact Lens Specification
Where a patient requests a copy of their own, or their child's spectacle prescription or contact lens specification this should be provided. It should be double checked for accuracy and signed by an optometrist. Such information may be collected or posted or faxed to the patient. It may also be emailed to their personal email address if they so request.

Contact Lens Specification
Where a 3rd party supplier requests the verification of a contact lens specification they should provide the following details:

- Patient's full name and address
- Full specification including parameters and power of the lenses
- An expiry date of the specification
- The name or registration number of the person signing the specification

The answer can only be yes or no; the details are correct or not. If the details are not correct, further information must not be supplied without the explicit consent of the patient. In that event the supplier should be told that a copy of the specification, with all the correct details, will be posted to the patient. The request, and the result, should be noted on the patient's record.

Requests from another optometrist for spec Rx information
In all cases you should be satisfied that the patient has consented to the transfer of the information. That may be obvious and implicit "the patient is on holiday elsewhere and has broken their glasses", but if not, ask to speak to the patient or for a signed consent to be faxed to us. The request should be noted on the patient's record.

Requests from another optometrist for clinical information
The optometrist should satisfy themselves that the request is for the clinical and health benefit of the patient and should conduct the phone conversation and provide the information themselves. They should also be satisfied that the patient has consented to the transfer of information.

Requests by us for clinical or spec Rx information.
These requests will be made by the optometrist personally. A signed consent should be held in case this is requested by the other party. If the information is not urgent the request may be made in writing using the form in the Appendix 1.

APPENDIX

Communicating Patient Identifiable Data

Patient data may be communicated in the following ways:

By ordinary 1st or 2nd class post

- This will be in a sealed envelope

By Fax

- This will be to a safe haven fax where possible. The cover sheet will

The cover sheet will state:

This fax contains proprietary confidential information some or all of which may be legally privileged and or subject to the provisions of privacy legislation. It is intended solely for the addressee. If you are not the intended recipient, you must not read, use, disclose, copy, print or disseminate the information contained within this fax. Please notify the author immediately by replying to this fax and then destroy the fax.

By email:

Patient consent is required for sending data that can identify an patient except where both sender and recipient have NHS emails ending in @nhs.net.

Verbally

- With care that confidentiality is maintained
- The recipient of the information is identified
- A note is made on the record.
- Information that could result in errors will be communicated in writing where possible

Appendix

A.N. Other Optometrists

Patient consent to the provision of information

To:

Patient:

Address:

I request that you provide A.N.Other Optometrists with the following information:

Signed . . . . . .

Date:

***N.B. Consent of the data subject* should NOT be used as the lawful basis for health records or employee records. It is most likely to be the lawful basis when data is processed for marketing purposes. Please note that there are other regulations to consider when using personal data for marketing. See Annex B.**

Annex A - EXAMPLE OF RECORD KEEPING IN TYPICAL PRACTICE (Update for your practice as necessary)

Name of Controller:
Address of Controller:
Telephone/Email:
Responsible person:

Category of personal data and data subject	Legal basis for processing personal data	Who these personal data are shared with	Time limits for erasure	Technical/organisational security measures to ensure level of security appropriate to risks
Patient records – including retinal photographs, referral letters etc.	Legitimate interest and for the purposes of health care	Registered health care professionals and those under their supervision	The NHS specifies 7 years or, in the case of children under 18, until their 25th birthday. College of Optometrists guidance is that it is best practice for records to be kept for 10 years.	Only registered health care staff have access to the complete patient record. All registered staff comply with GOC standards, which ensure they respect patient confidentiality. Paper records are kept securely. Electronic data is password protected, employees can only access the information essential for their role, all employees have passwords so there is an audit of any changes made, there is also a back-up system that means data can be restored. All anti-virus software and other software are kept up to date.
Customer records – e.g. direct debit/payment details	Legitimate interest	The data subject's bank	Kept for tax purposes and future claims/information	Paper records are kept securely. Electronic data is password protected, employees can only access the information essential for their role and receive appropriate training for their role. All employees have passwords so there is an audit of any changes made, there is also a back-up system that means data can be restored. All anti-virus software and other software are kept up to date.

Staff records – includes bank details, NI number, and other personal information	Performance of a contract with the data subject or to take steps to enter into a contract and processing is necessary for carrying out obligations as an employer	HR (including payroll) and senior management only	Kept for tax purposes and future claims/information	Paper records are kept securely. Electronic data is password protected, employees can only access the information essential for their role and receive appropriate training for their role. All employees have passwords so there is an audit of any changes made, there is also a back-up system that means data can be restored. All anti-virus software and other software are kept up to date.

Annex B – LAWFUL BASES FOR PROCESSING PERSONAL DATA (Update for your practice as necessary)

Practices and businesses will need to have at least one lawful basis for processing personal data. This means having a legal basis for each processing activity.

Legal basis for processing personal data	Notes
1. Consent of the data subject	Should NOT be used as the lawful basis for health records or employee records. Most likely to be the lawful basis when data is processed for marketing purposes. Please note that there are other regulations to consider when using personal data for marketing. For more details on marketing please also see the ICO guidance on direct marketing. Also note that the EU is giving consideration to reforming the existing e-Privacy Directive, with the aim of harmonising it with the GDPR.
2.Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract	Employment contracts and data held on employees that is consistent with the contract of employment.
3.Processing is necessary for compliance with a legal obligation	Might be used by a practice, for example to comply with tax law.
4.Processing is necessary to protect the vital interests of a data subject or another person	Less likely that practices will rely on this condition.
5.Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller	Less likely that practices will rely on this condition.
6.Necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject (Note that this condition is not available to processing carried out by public authorities in the performance of their tasks).	Likely to be the lawful basis for most personal data held by practices (please note that health records cannot be processed solely on this lawful basis as they are also a special category of data – see below)
There are additional requirements for anybody processing the following special categories of data: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited, unless this is done as part of any of the following provisions:	
7. Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law	Less likely that practices will rely on this condition.
8. Processing is necessary for carrying out obligations under employment, social security or social protection law, or a collective agreement	Practices might rely on this condition.

9. Processing is necessary to protect the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent	Less likely that practices will rely on this condition.
10. Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent	Less likely that practices will rely on this condition.
11. Processing relates to personal data manifestly made public by the data subject	Less likely that practices will rely on this condition.
12. Processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity	It is possible that health care records and other special categories of data might have to be shared in this context – e.g. the final Data Protection Act in the UK might clarify sharing of patient records with regulators.
13. Processing is necessary for reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards	Less likely that practices will rely on this condition.
14. Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional	Practices will rely on this provision when processing health records.
15. Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices	Less likely that practices will rely on this condition.
16. Processing is necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1)	Less likely that practices will rely on this condition.

Table 1: Legal basis for processing personal data, modified ICO table: source https://ico.org.uk/for-organisations/data-protection-reform/overview-of-thegdpr/key-areas-to-consider/

GUIDANCE

Annex C - INDIVIDUAL RIGHTS The table below sets out the eight rights individuals will have under the new law

Right	What does this mean in my practice or business?
The right to be informed	♣ Be transparent about how you use personal data by letting patients and customers have access to 'fair processing information' – e.g. by using a privacy notice. ♣ Supply this information in a way that is: concise, transparent, intelligible and easily accessible; written in clear and plain language, particularly if addressed to a child; and free of charge. ♣ For details on what you might include in a privacy statement see section 2.6 (http://www.opticalconfederation.org.uk/downloads/data-protection-and-gdpr-guidance--final.pdf)
The right of access	♣ If you process personal data then individuals – e.g. customers, patients, staff – can ask what you are processing and why, and ask for copies of that data, see Subject Access Requests.
The right to rectification	♣ Individuals can ask you to rectify personal data if it is inaccurate or incomplete. ♣ Respond to such requests within one month, although if it is a complicated request you might be able to extend this by two months.
The right to erasure	♣ This is also known as 'the right to be forgotten' – e.g. a person might be able to ask you to delete or remove personal data you hold on them. ♣ This applies where there is no compelling reason for its continued processing. It is therefore not applicable where there is a duty to keep accurate records – e.g. keeping health and employee records is often best practice and a requirement in case of a legal claim etc.
The right to restrict processing	♣ A customer has the right to 'block' or suppress you processing their data in certain circumstances. This is unlikely to apply in a typical optical practice. ♣ If there is a basis for a customer to exercise this right then you can store the personal data, but not further process it.
The right to data portability	♣ This is unlikely to apply to optical practices because it applies when processing is carried out by automated means.
The right to object	♣ Individuals can object to you processing their personal data in certain circumstances ♣ If you used "legitimate interest" as the lawful basis for processing personal data and an individual objects you must stop processing data unless you can a) demonstrate how your legitimate interests override the interests, rights and freedoms of the individual or b) you are processing the data for the establishment, exercise or defence of legal claims ♣ If an individual objects to you

	processing personal data for direct marketing, you must stop processing data for that purpose.
The right not to be subject to automated decision making including profiling	♣ This is unlikely to apply in optical settings. ♣ If you would like to learn more about this particular right, please see pages 30-32 ICO, 21 Nov 2017, Guide to the General Data Protection Regulations Version 1

Table 3: An individual's rights under new data protection law, adapted for hearing practice from pages 16-30 of the ICO, 21 Nov. 2017, Guide to the General Data Protection Regulations (GDPR)