EYE SURGERY PATIENT PRIVACY NOTICE

This Privacy Notice:

- provides you with a detailed overview of how we will manage your data, from the point at which it is gathered and onwards.
- will give you all the details you need on how we use your information, and how we will comply with the law.
- sets out your rights in respect of your personal information, and how to exercise them. You can, for instance, seek access to your medical information, object to us using your information in particular ways and request rectification of any information which is inaccurate.

We are also open to improvement; if you have any feedback on this notice contact our office.

Introduction

1. This Privacy Notice sets out details of the information that I, as a clinician responsible for your treatment (and including my medical secretaries), may collect from you and how that information may be used. Please take your time to read this Privacy Notice carefully.

About me

2. In this Privacy Notice I use "**I**" or "**mine**" or "**my**" to refer to me as the clinician who is using your personal information.

3. In the event that you have any queries, comments or concerns in respect of the manner in which I have used, or potentially will use, your personal information then please contact the office directly.

Your personal data

4. I am a Data Controller in respect of the personal information which I hold about you. This will mainly relate to your medical treatment but will be likely to also include other information such as financial data in relation to billing. I must comply with the data protection legislation and relevant guidance when handling your personal information, and so must any medical secretary who assists me in an administrative capacity. Your personal data may include any images taken in relation to your treatment which must be managed in accordance with the law, this Privacy Notice guidance from the General Medical Council, and British Medical Association.

5. I will provide your treatment from a NHS Hospital provider or an independent healthcare hospital provider, and, in due course, it may be necessary for the NHS or the independent provider to also process your personal data. I will do so in accordance with the law, the principles of this Privacy Notice and to the extent that it is necessary to do so. This could be where the NHS or the other independent provider needs to arrange other healthcare services as part of your treatment, such as nursing or dietician advice, or support other aspects of the treatment which I provide to you. In

that case, the NHS or the other independent provider will become a joint Data Controller in respect of your personal information and you will be provided with a copy of their Privacy Notice which sets out how they will manage that information.

6. Your personal information will be handled in accordance with the principles set out within this Privacy Notice. This means that whenever I use your personal data, I will only do so as set out in this Privacy Notice. From time to time, I may process your personal information at a non-NHS or a non-independent provider site (medical or non-medical), as may my medical secretary.

What personal information do I collect and use from patients?

7. I will use “special categories of personal information” (previously known as "sensitive personal data") about you, such as information relating to your physical and mental health.

8. If you provide personal information to me about other individuals (including medical or financial information) you should inform the individual about the contents of this Privacy Notice. I will also process such information in accordance with this Privacy Notice.

9. In addition, you should note that in the event you amend data which I already hold about you (for instance by amending a pre-populated form) then I will update our systems to reflect the amendments. Our systems will continue to store historical data.

Personal information

10. As one of my patients, the personal information I hold about you may include the following:

    a) Name
    b) Contact details, such as postal address, email address and telephone number (including mobile number)
    c) Financial information, used to pay us including insurance policy details if applicable
    d) Occupation
    e) Emergency contact details, including next of kin
    f) Background referral details

Special Categories Personal Information

11. As one of my patients, I will hold information relating to your medical treatment which is known as a special category of personal data under the law, meaning that it must be handled even more sensitively. This may include the following:

    a) Details of your current or former physical or mental health, including information about any

healthcare you have received from other healthcare providers such as GPs, dentists or hospitals (private and/or NHS), which may include details of clinic and hospital visits, as well as medicines administered. I will provide further details below on the manner in which I handle such information.

b) Details of services you have received from me
c) Details of your nationality, race and/or ethnicity
d) Details of your religion
e) Details of any genetic data or biometric data relating to you

12. The confidentiality of your medical information is important to me, and I make every effort to prevent unauthorised access to and use of information relating to your current or former physical and mental health (or indeed any of your personal information more generally). In doing so, I will comply with UK data protection law, including the Data Protection Act 2018 and all applicable medical confidentiality guidelines issued by professional bodies including, but not limited to, the General Medical Council and the Nursing and Midwifery Council.

13. From 25 May 2018, the current Data Protection Act will be replaced by the EU General Data Protection Regulation (**GDPR**) and a new Data Protection Act. All uses of your information will comply with the GDPR and the new Data Protection Act from that date onwards

How do I collect your information?

14. I may collect personal information from a number of different sources including, but not limited to:

a) GPs
b) Optometrists
c) Other hospitals, both NHS and private (including Spire/other independent provider)
d) Other clinicians (including their medical secretaries)
e) Commissioners of healthcare services

Directly from you

15. Information may be collected directly from you when:

a) You enter into a contract with me or the NHS or another independent provider for the provision of healthcare services
b) You use those services
c) You complete enquiry forms on the NHS or on an independent provider website
d) You submit a query to me including by email or by social media
e) You correspond with me by letter, email, telephone or social media.

From other healthcare organisations

16. My patients will usually receive healthcare from other organisations, and so in order to provide you with the best treatment possible I may have to collect personal information about you from them. These may include:

    a) Medical records from your GP
    b) Medical records from other clinicians (including their medical secretaries)
    c) Medical records from the NHS or any private healthcare organisation

17. Medical records include information about your diagnosis, clinic and hospital visits and medicines administered.

From third parties

18. As detailed in the previous section, it is often necessary to seek information from other healthcare organisations. I may also collect information about you from third parties when:

    a) You are referred to me for the provision of services including healthcare services
    b) I liaise with your current or former employer, health professional or other treatment or benefit provider
    c) I liaise with your family
    d) I liaise with your insurance policy provider
    e) I deal with experts (including medical experts) and other service providers about services you have received or are receiving from me
    f) I deal with NHS health service bodies about services you have received or are receiving from us
    g) I liaise with credit reference agencies
    h) I liaise with debt collection agencies
    i) I liaise with Government agencies, including the Ministry of Defence, the Home Office and HMRC

How will I communicate with you?

19. I may communicate with you in a range of ways, including by telephone, SMS, email, and / or post. If I contact you using the telephone number(s) which you have provided (landline and/or mobile), and you are not available which results in the call being directed to a voicemail and/or answering service, I may leave a voice message on your voicemail and/or answering service as appropriate, and including only sufficient basic details to enable you to identify who the call is from, very limited detail as to the reason for the call and how to call me back.

20. However:
    a) to ensure that I provide you with timely updates and reminders in relation to your healthcare or tests or invoicing information. I may communicate with you by email encrypted or unencrypted email, text messaging or telephone as expressed by you under preferences in the patient registration form. The first time I send you any important encrypted email that I am not also sending by post or which requires action to be taken, I will endeavour to contact you separately to ensure that you are able to access the encrypted email you are sent.

21. Please note that although providing your mobile number and email address and stating a preference to be communicated by a particular method will be taken as an affirmative confirmation that you are happy for us to contact you in that manner, I am not relying on your consent to process your personal data in order to correspond with you about your treatment. As set out further below, processing your personal data for those purposes is justified on the basis that it is necessary to provide you with healthcare service.

What are the purposes for which your information is used?

22. I may 'process' your information for a number of different purposes, which is essentially the language used by the law to mean using your data. Each time I use your data I must have a legal justification to do so. The particular justification will depend on the purpose of the proposed use of your data. When the information that we process is classed as a “special category of personal information”, I must have a specific additional legal justification in order to use it as proposed.

23. Generally I will rely on the following legal justifications, or 'grounds':

    a) Taking steps at your request so that you can enter into a contract with me to receive healthcare services from us.
    b) For the purposes of providing you with healthcare pursuant to a contract between you and I. I will rely on this for activities such as supporting your medical treatment or care and other benefits, supporting your nurse, carer or other healthcare professional and providing other services to you.
    c) I have an appropriate business need to process your personal information and such business need does not cause harm to you. I will rely on this for activities such as quality assurance, maintaining my business records, monitoring outcomes and responding to any complaints.
    d) I have a legal or regulatory obligation to use such personal information.
    e) I need to use such personal information to establish, exercise or defend my legal rights.
    f) You have provided your consent to my use of your personal information.

24. Note that failure to provide your information further to a contractual requirement with me may mean that I am unable to set you up as a patient or facilitate the provision of your healthcare.

25. I provide further detail on these grounds in the sections below.

Appropriate business needs

26. One legal ground for processing personal data is where I do so in pursuit of legitimate interests and those interests are not overridden by your privacy rights. Where I refer to use for my appropriate business needs, I am relying on this legal ground.

The right to object to other uses of your personal data

27. You have a range of rights in respect of your personal data, as set out in detail in sections 69 – 90. This includes the right to object to me using your personal information in a particular way (such as sharing that information with third parties), and I must stop using it in that way unless specific exceptions apply. This includes, for example, if it is necessary to defend a legal claim brought against me, or it is otherwise necessary for the purposes of your ongoing treatment.

You will find details of my legal grounds for each of our processing purposes below. I have set out individually those purposes for which I will use your personal information, and under each one I set out the legal justifications, or grounds, which allow me to do so. You will note that I have set out a legal ground, as well as an 'additional' legal ground for special categories of personal information. This is because I have to demonstrate additional legal grounds where using information which relates to a person's healthcare, as I will be the majority of the times I use your personal information.

Purpose 1: To set you up as my patient, including carrying out fraud, credit, anti-money laundering and other regulatory checks

28. As is common with most business, I have to carry out necessary checks in order for you to become a patient. These include standard background checks, which I cannot perform without using your personal information.

29. **Legal ground:** Taking the necessary steps so that you can enter into a contract with me for the delivery of healthcare.

30. **Additional legal ground for special categories of personal information**: The use is necessary for reasons of substantial public interest, and it is also in my legitimate interests to do so.

Purpose 2: To provide you with healthcare and related services

31. Clearly, the reason you come to me is to provide you with healthcare, and so I have to use your personal information for that purpose.

32. **Legal grounds:**
    a) Providing you with healthcare and related services
    b) Fulfilling my contract with you for the delivery of healthcare

33. **Additional legal grounds for special categories of personal information**:
    a) I need to use the data in order to provide healthcare services to you
    b) The use is necessary to protect your vital interests where you are physically or legally incapable of giving consent

Purpose 3: For account settlement purposes

34. I will use your personal information in order to ensure that your account and billing is fully accurate and up-to-date

35. **Legal grounds:**
    a) My providing you healthcare and other related services
    b) Fulfilling my contract with you for the delivery of healthcare
    c) My having an appropriate business need to use your information which does not overly prejudice you
    d) Your consent

36. **Additional legal grounds for special categories of personal information**:
    a) I need to use the data in order to provide healthcare services to you
    b) The use is necessary in order for me to establish, exercise or defend my legal rights
    c) Your consent

Purpose 4: For medical audit/research purposes

<u>Clinical audit</u>

37. I may process your personal data for the purposes of local clinical audit – i.e. an audit carried out by myself or my direct team for the purposes of assessing outcomes for patients and identifying improvements which could be made for the future. I am able to do so on the basis of my legitimate interest and the public interest in statistical and scientific research, and with appropriate safeguards in place. You are, however, entitled to object to my using your personal data for this purpose, and as a result of which I would need to stop doing so. Please note that I will use anonymised data. If you would like to raise such an objection, then please contact me using the details provided in paragraph 3 above.

38. I may also be asked to share information with U.K. registries for which ethical approval is not necessarily required but which form part of the National Clinical Audit programme, hosted by NHS

England and who provide a list of National Clinical Audit and Clinical Outcome Review programmes and other quality improvement programmes which we should prioritise for participation. I may do so without your consent provided that the particular audit registry has received statutory approval, or where the information will be provided in a purely anonymous form, otherwise your consent will be needed and either I will seek this from you or the registry themselves will do so. The registries which I regularly share data with are Medisoft and the RCOphth National Ophthalmology Database (NOD).

Medical research

39. I may also be asked to participate in medical research and share data with ethically approved third party research organisations.

40. I will share your personal data only to the extent that it is necessary to do so in assisting research and as permitted by law. Some research projects will have received statutory approval such that consent may not be required in order to use your personal data. In those circumstances, your personal will be shared on the basis that:

Legal grounds:

a) I have a legitimate interest in helping with medical research and have put appropriate safeguards in place to protect your privacy

Additional legal grounds for special categories of personal information:

b) The processing is necessary in the public interest for statistical and scientific research purposes

41. In the event that consent is required then either I will seek this from you, or the research agency will do so.

Purpose 5: Communicating with you and resolving any queries or complaints that you might have.

42. From time to time, patients may raise queries, or even complaints, with me or other independent providers and I take those communications very seriously. It is important that I am able to resolve such matters fully and properly and so I, as well as independent providers will need to use your personal information in order to do so.

43. **Legal grounds:**

a) Providing you with healthcare and other related services

b) Having an appropriate business need to use your information which does not overly prejudice you

44. **Additional legal grounds for special categories of personal information**:
    a) The use is necessary for the provision of healthcare or treatment pursuant to a contract with a health professional
    b) The use is necessary in order for me to establish, exercise or defend my legal rights

Purpose 6: Communicating with any other individual that you ask us to update about your care and updating other healthcare professionals about your care.

45. In addition, other healthcare professionals or organisations may need to know about your treatment in order for them to provide you with safe and effective care, and so I may need to share your personal information with them. Further details on the third parties who may need access to your information is set out at section 56 below.

46. **Legal grounds:**
    a) Providing you with healthcare and other related services
    b) I have a legitimate interest in ensuring that other healthcare professionals who are routinely involved in your care have a full picture of your treatment

47. **Additional legal ground for special categories of personal information:**
    a) I need to use the data in order to provide healthcare services to you
    b) The use is necessary for reasons of substantial public interest under UK law
    c) The use is necessary in order for me to establish, exercise or defend my legal rights

48. I also participate in initiatives to monitor safety and quality, helping to ensure that patients are getting the best possible outcomes from their treatment and care. The Competition and Markets Authority Private Healthcare Market Investigation Order 2014 established the Private Healthcare Information Network ("**PHIN**"), as an organisation who will monitor outcomes of patients who receive private treatment. Under Article 21 of that Order, I am required to provide PHIN with information related to your treatment, including your NHS Number in England and Wales, CHI Number in Scotland or Health and Care Number in Northern Ireland), the nature of your procedure, whether there were any complications such as infection or the need for readmission/admission to a NHS facility and also the feedback you provided as part of any PROMs surveys. PHIN will use your information in order to share it with the NHS, and track whether you have received any follow-up treatment. I will only share this information with PHIN if you have provided your consent for me to do so.

49. The records that I share may contain personal and medical information about patients, including you. PHIN, like me, will apply the highest standards of confidentiality to personal information in accordance with data protection laws and the duty of confidentiality. Any information that is

published by PHIN will always be in anonymised statistical form and will not be shared or analysed for any purpose other than those stated. Further information about how PHIN uses information, including its Privacy Notice, is available at www.phin.org.uk.

Purpose 7: Complying with our legal or regulatory obligations, and defending or exercising our legal rights

50. As a provider of healthcare, I am subject to a wide range of legal and regulatory responsibilities which is not possible to list fully here. I may be required by law or by regulators to provide personal information, and in which case I will have a legal responsibility to do so. From time to time, clinicians are unfortunately also the subject of legal actions or complaints. In order to fully investigate and respond to those actions, it is necessary to access your personal information (although only to the extent that it is necessary and relevant to the subject-matter).

51. **Legal grounds:**
    a) The use is necessary in order for us to comply with our legal obligations

52. **Additional legal ground for special categories of personal information:**
    a) I need to use the data in order for others to provide informed healthcare services to you
    b) The use is necessary for reasons of the provision of health or social care or treatment or the management of health or social care systems
    c) The use is necessary for establishing, exercising or defending legal claims

53. I am also required by law to conduct audits of health records, including medical information, for quality assurance purposes. Your personal and medical information will be treated in accordance with guidance issued by the Care Quality Commission (England), Health Inspectorate Wales and Healthcare Improvement Scotland

Purpose 8: Managing my business operations such as maintaining accounting records, analysis of financial results, internal audit requirements, receiving professional advice (e.g. tax or legal advice)

54. In order to do this, I will not need to use your special categories of personal information and so I have not identified the additional ground to use your information for this purpose.

55. **Legal grounds**:
    a) My having an appropriate business need to use your information which does not overly prejudice you
    b) You have provided your consent

Disclosures to third parties:

56. I may disclose your information to the third parties listed below for the purposes described in this Privacy Notice. This might include:

    a) An Optometrist
    b) A doctor, nurse, carer or any other healthcare professional involved in your treatment
    c) Other members of support staff involved in the delivery of your care, like receptionists and porters
    d) Anyone that you ask me to communicate with or provide as an emergency contact, for example your next of kin or carer
    e) NHS organisations, including NHS Resolution, NHS England, Department of Health
    f) Other private sector healthcare providers
    g) Your GP
    h) Your dentist
    i) Other clinicians (including their medical secretaries)
    j) Third parties who assist in the administration of your healthcare, such as insurance companies
    k) Consultants Eye Surgeons Partnership (CESP), who facilitate our billing.
    l) Private Healthcare Information Network
    m) National and other professional research/audit programmes and registries, as detailed under purpose 4 above
    n) Government bodies, including the Ministry of Defence, the Home Office and HMRC
    o) Our regulators, like the Care Quality Commission, Health Inspectorate Wales and Healthcare Improvement Scotland
    p) The police and other third parties where reasonably necessary for the prevention or detection of crime
    q) Our insurers
    r) Debt collection agencies
    s) Credit referencing agencies
    t) Our third-party services providers such as IT suppliers, actuaries, auditors, lawyers, marketing agencies, document management providers and tax advisers
    u) Selected third parties in connection with any sale, transfer or disposal of our business
    v) I may also use your personal information to provide you with information about products or services which may be of interest to you where you have provided your consent for me to do so.

Automated Decision Making

57. An automated decision is a decision made by computer without any human input, and there will be no automated decision-making in relation to your treatment or other decisions which will produce

legal or similarly significant effects.

How long do I keep personal information for?

58. I will only keep your personal information for as long as reasonably necessary to fulfil the relevant purposes set out in this Privacy Notice and in order to comply with my legal and regulatory obligations.

59. If you would like further information regarding the periods for which your personal information will be stored, please contact me at Eye Surgery, PO Box 59529, London, SE21 9AY.

International data transfers

60. I (or third parties acting on my behalf) may store or process information that we collect about you in countries outside the European Economic Area ("**EEA**"). Where I make a transfer of your personal information outside of the EEA I will take the required steps to ensure that your personal information is protected.

    a) To the extent that it is necessary to do so, I may transfer your personal data outside of the EEA to:

61. I will only do so to the extent that it is relevant and necessary. Under certain circumstances, I may request your consent for such a transfer.

62. If you would like further information regarding the steps I take to safeguard your personal information, please contact me using the details provided in section 3 above.

63. Please note that we have listed above the current common transfers of personal data outside of the EEA but it may be necessary, in future, to transfer such data for other purposes. In the event that it is necessary to do so, we will update this Privacy Notice.

Your rights

64. Under data protection law you have certain rights in relation to the personal information that I hold about you. These include rights to know what information I hold about you and how it is used. You may exercise these rights at any time by contacting me using the details provided at section 3 above.

65. There will not usually be a charge for handling a request to exercise your rights.

66. If I cannot comply with your request to exercise your rights, we will usually tell you why.

67. There are some special rules about how these rights apply to health information as set out in legislation including the Data Protection Act (current and future), the General Data Protection Regulation as well as any secondary legislation which regulates the use of personal information.

68. If you make a large number of requests or it is clear that it is not reasonable for me to comply with a request then we do not have to respond. Alternatively, I can charge for responding.

Your rights include:

The right to access your personal information

69. You are usually entitled to a copy of the personal information I hold about you and details about how I use it.

70. Your information will usually be provided to you in writing, unless otherwise requested. If you have made the request electronically (e.g. by email) the information will be provided to you by electronic means where possible.

71. Please note that in some cases I may not be able to fully comply with your request, for example if your request involves the personal data of another person and it would not be fair to that person to provide it to you.

72. You are entitled to the following under data protection law.
    1. Under Article 15(1) of the GDPR I must usually confirm whether I have personal information about you. If I do hold personal information about you, I usually need to explain to you:
        i. The purposes for which I use your personal information
        ii. The types of personal information I hold about you
        iii. Who your personal information has been or will be shared with, including in particular organisations based outside the EEA.
        iv. If your personal information leaves the EU, how I will make sure that it is protected
        v. Where possible, the length of time I expect to hold your personal information. If that is not possible, the criteria I use to determine how long I hold your information for
        vi. If the personal data I hold about you was not provided by you, details of the source of the information
        vii. Whether I make any decisions about you solely by computer and if so details of how those decision are made and the impact they may have on you
        viii. Your right to ask me to amend or delete your personal information

ix. Your right to ask me to restrict how your personal information is used or to object to my use of your personal information

x. Your right to complain to the Information Commissioner's Office

2. I also need to provide you with a copy of your personal data, provided specific exceptions and exemptions do not apply.

The right to rectification

73. I take reasonable steps to ensure that the information I hold about you is accurate and complete. However, if you do not believe this is the case, you can ask me to update or amend it.

The right to erasure (also known as the right to be forgotten)

74. I may update this Privacy Notice from time to time to ensure that it remains accurate, and the most up-to-date version can always be found on my webpage at www.eyesurgeryltd.co.uk. In the event that there are any material changes to the manner in which your personal information is to be used then I will provide you with an updated copy of this Privacy Notice.

75. In some circumstances, you have the right to request that I delete the personal information I hold about you. However, there are exceptions to this right and in certain circumstances I can refuse to delete the information in question. In particular, for example, I do not have to comply with your request if it is necessary to keep your information in order to perform tasks which are in the public interest, including public health, or for the purposes of establishing, exercising or defending legal claims.

The right to restriction of processing

76. In some circumstances, I must "pause" our use of your personal data if you ask me to do so, although I do not have to comply with all requests to restrict my use of your personal information. In particular, for example, I do not have to comply with your request if it is necessary to keep your information in order to perform tasks which are in the public interest, including public health, or for the purposes of establishing, exercise or defending legal claims.

The right to data portability

77. In some circumstances, I must transfer personal information that you have provided to you or (if this is technically feasible) another individual/ organisation of your choice. The information must be transferred in an electronic format.

The right to withdraw consent

78. In some cases, I may need your consent in order for my use of your personal information to comply with data protection legislation. Where we do this, you have the right to withdraw your consent to further use of your personal information. You can do this by contacting me using the details provided at section 3 above.

The right to complain to the Information Commissioner's Office

79. You can complain to the Information Commissioner's Office if you are unhappy with the way that I have dealt with a request from you to exercise any of these rights, or if you think I have not complied with our legal obligations.

80. More information can be found on the Information Commissioner's Office website: https://ico.org.uk/

81. Making a complaint will not affect any other legal rights or remedies that you have.

National Data Opt-Out Programme

82. NHS Digital is currently developing a national programme which will go live on 25 May 2018, pursuant to which all patients will be able to log their preferences as to sharing of their personal information. All health and care organisations will be required to uphold patient choices, but only from March 2020. In the meantime, you should make me aware directly of any uses of your data to which you object.

Updates to this Privacy Notice

83. I may update this Privacy Notice from time to time to ensure that it remains accurate. In the event that these changes result in any material difference to the manner in which I process your personal data then I will provide you with an updated copy of the Policy.

84. This Privacy Notice was last updated on 29/4/19