

## **Patient Privacy Notice for GDPR – Nick Linton**

### **Executive summary**

1. As your treating clinician and therefore custodian of personal data relating to your medical treatment, I must only use that personal data in accordance with all applicable law and guidance. This Privacy Notice provides you with a detailed overview of how I will manage your personal data from the point at which it is gathered and onwards, and how that complies with the law. I will use your personal data for a variety of purposes including, but not limited to, providing you with care and treatment, sharing it with other medical professionals and research/clinical audit programmes. I may also be using your personal data in the context of carrying out an assessment of your condition as part of a medico-legal claim you are considering or already bringing against another healthcare provider or in another context.
2. In addition, you have a number of rights as a data subject. You can, for instance, seek access to your medical information, object to me using your personal data in particular ways, request rectification of any information which is inaccurate or deletion of personal data which is no longer required (subject to certain exceptions). This Privacy Notice also sets out your rights in respect of your personal data, and how to exercise them.
3. For ease of reference, this Notice is broken into separate sections below with headings which will help you to navigate through the document.

### **Introduction**

1. This Privacy Notice sets out details of the information (personal data) that I, as a clinician responsible for your treatment and assessment (and including my medical secretaries), may collect from you and how that personal data 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 has your personal data.
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 data then you should contact me directly and I would be happy to discuss further. I can be contacted via [www.nicklinton.org](http://www.nicklinton.org).

## **Your personal data**

4. I am a Data Controller in respect of your personal data which I hold about you. This will mainly relate to your medical treatment and condition, but will be likely to also include other personal data such as financial data in relation to billing. I must comply with the data protection legislation and relevant guidance when handling your personal data, and so must any medical secretary who assists me in an administrative capacity.
5. Your personal data may include any images taken in relation to your treatment which must not only be managed in accordance with the law and this Privacy Notice but also all applicable professional standards including guidance from the General Medical Council. In many circumstances, particularly where the imaging is diagnostic and relates to internal organs, I am unlikely to require your consent. The images generated will form part of your patient record, and be managed in accordance with the principles set out in this Privacy Notice. In the event that the imaging relates to an external part of the body, or I would like to use any imaging for secondary purposes other than your care (for instance, marketing) then I will seek your specific consent to do so.
6. I will provide your treatment from a Spire Healthcare Hospital or other independent provider and, in due course, it may be necessary for Spire and/or other independent provider to also process your personal data. They will do so in accordance with the law and the principles of their own Privacy Notice. Spire and/or other independent provider would typically start processing your personal data from the point at which you are booked for an appointment or otherwise registered as a patient on their system and may entail circumstances in which they need 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, Spire and/or other independent provider will become a joint Data Controller in respect of your personal data from the point of your registration as a patient of theirs onwards, and it is their responsibility to provide you with a copy of their Privacy Notice which sets out how they will manage that personal data.
7. Your personal data 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 data at a non-Spire site (medical or non-medical), as may my medical secretary (more details are provided in the next section).

## **Medical secretarial services**

8. My medical secretary is employed by Private Practice management. She/he will only use your personal data in line with my instructions.
9. Private Practice Management Ltd employs my medical secretary. My medical secretary uses Spire

computers only for her correspondence regarding patients, and a Spire telephone. We both use DGL software, which is on a private cloud to store all patient records. As a "Private Cloud", only users with whom we have a direct business relationship have access. The data centre used by DGL is fully UKAS accredited for ISO 9001 Quality Management Systems, and certified for ISO 27001 for Data Security. Both DGL and the data centre are registered and comply with the Data Protection Act. Data centre staff only have access to the servers for the purpose of maintenance and have no access to patient data. DGL only use dedicated servers. All servers are exclusive to DGL with no public access and are not shared by other companies. All access to the servers is restricted using RSA SecurID two-factor authentication. This requires a valid username (NOT the same as their email address), a complex password, PIN number AND a six digit security code from their RSA SecurID keyfob which changes every 60 seconds. All communication between the users and the servers is encrypted to the highest level available to the client. All traffic to the servers is filtered through a pair of enterprise level SonicWall devices, which scan all communications for viruses/malware and have state of the art Intrusion Prevention & Detection (IPD) systems to detect and prevent hacking attempts. It is impossible for a user to grant access to anyone in the outside world, either accidentally or intentionally.

#### **What personal data do I collect and use from patients?**

10. I will use "special categories of personal data" (previously known as "sensitive personal data") about you, such as information relating to your physical and mental health.
11. If you provide personal data 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 personal data in accordance with this Privacy Notice.
12. 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 personal data.

#### **Personal data**

13. As one of my patients, the personal data 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, such as credit card details used to pay us and insurance policy details
  - d) Occupation

- e) Emergency contact details, including next of kin
- f) Background referral details

### **Special Categories of Personal Data**

14. As one of my patients, I will hold personal data 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 personal data 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. This may also include details of previous treatment you have received from other healthcare providers in circumstances where medical negligence is alleged, or being investigated, against that third party provider. It may also include the relevant medical history relating to any medico-legal claim that you are pursuing. I will provide further details below on the manner in which I handle such personal data.
- 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
- f) Data concerning your sex life and/or sexual orientation

15. The confidentiality of your medical information is important to me, and I make every effort to prevent unauthorised access to and use of personal data relating to your current or former physical and mental health (or indeed any of your personal data more generally). In doing so, I will comply with UK data protection law, including the Data Protection Act 2018, the EU General Data Protection Regulation 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.

### **How do I collect your personal data?**

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

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

- g) Solicitors or other third parties acting on your behalf in connection with medico-legal proceedings

### **Directly from you**

17. Personal data may be collected directly from you when:

- a) You enter into a contract with me or Spire and/or other independent provider for the provision of healthcare services
- b) You use those services
- c) You complete enquiry forms on the Spire/other 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 or telephone

### **From other healthcare organisations**

18. 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 data 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 your dentist
- d) Medical records from the NHS or any private healthcare organisation

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

### **From third parties**

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

- a) You are referred to me for the provision of services including healthcare services
- b) I deal and liaise with, as relevant, referring third party agencies such as solicitors or insurers acting on your behalf in connection with medico-legal proceedings, and who refer you to me for the purposes of an assessment of your condition.
- c) I liaise with your current or former employer, health professional or other treatment or benefit provider
- d) I liaise with your family
- e) I liaise with your insurance policy provider
- f) I deal with experts (including medical experts) and other service providers about services

you have received or are receiving from me

- g) I deal with NHS health service bodies about services you have received or are receiving from us
- h) I liaise with credit reference agencies
- i) I liaise with debt collection agencies
- j) I liaise with Government agencies, including the Ministry of Defence, the Home Office and HMRC

### **How will I communicate with you?**

21. 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.

22. However:

- a) to ensure that I provide you with timely updates and reminders in relation to your healthcare (including basic administration information and appointment information (including reminders)), I may communicate with you by SMS and/or unencrypted email (where you have provided me with your SMS or email address).
- b) to provide you with your medical information (including test results and other clinical updates) and/or invoicing information, I may communicate with you by email (which will be encrypted) where you have provided me with your email address. 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.

23. 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?**

24. I may 'process' your personal data for a number of different purposes, which is essentially the language used by the law to mean using your personal data. Each time I use your personal data I must have a legal justification to do so. The particular justification will depend on the purpose of the proposed use of your personal data. When the personal data that I process is classed as a "special

category of personal data”, I must have a specific additional legal justification in order to use it as proposed.

25. 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 data 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 data to establish, exercise or defend my legal rights.
- f) You have provided your consent to my use of your personal data.
- g) I need to use personal data to assist my assessment of your condition in the context of alleged or potential medical negligence against another healthcare provider, or any another type of medico-legal claim that you may be pursuing.

26. Note that failure to provide your personal data 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.

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

### ***Appropriate business needs***

28. 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**

29. You have a number of rights in respect of your personal data, as set out in detail in sections below. This includes the right to object to me using your personal information in a particular way (such as sharing that personal data 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 data, 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 data. This is because I have to demonstrate additional legal grounds where using personal data which relates to a person's healthcare, as I will be the majority of the times I use your personal data.

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

30. As is common with most business, I have to carry out necessary checks in order for you to become a patient (which includes becoming a patient for the purposes of a medico-legal assessment). These include standard background checks, which I cannot perform without using your personal data.

31. **Legal ground:** Taking the necessary steps so that you can enter into a contract with me for the delivery of healthcare and/or a medico-legal assessment.

**32. Additional legal ground for special categories of personal data:**

- a) The use is necessary for reasons of substantial public interest, and it is also in my legitimate interests to do so (namely the provision of private healthcare to you).
- b) The use is necessary for the purposes of enabling you to establish, exercise or defend legal claims.

***Purpose 2: To provide you with healthcare and related services***

33. Clearly, the main reason you come to me is likely to seek healthcare, and so I have to use your personal data for that purpose. You may also come to me for an assessment of your condition to assist in the investigation of potential medical negligence against a third party healthcare provider or any other kind of medico-legal claim you are pursuing.

**34. Legal grounds:**

- a) Providing you with healthcare and related services
- b) Fulfilling my contract with you for the delivery of healthcare

**35. Additional legal grounds for special categories of personal information:**

- a) I need to use the personal 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
- c) The use is necessary for the purposes of enabling you to establish, exercise or defend legal claims.



### ***Purpose 3: For account settlement purposes***

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

#### **37. 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 personal data which does not overly prejudice you
- d) Your consent

#### **38. Additional legal grounds for special categories of personal data:**

- a) I need to use the personal 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**

#### **Clinical audit**

39. 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. If you would like to raise such an objection then please contact me using the details provided in paragraph 3 above.

40. I may also be asked to share personal data 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 registry which I regularly share personal data with is the British Spinal Registry.

## **Medical research**

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

42. 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 data 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 data:**

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

43. 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.***

44. From time to time, patients may raise queries, or even complaints, with me and [Spire/other independent provider] 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 [Spire/other independent provider] will need to use your personal data in order to do so.

### **45. Legal grounds:**

- a) Providing you with healthcare and other related services
- b) Having an appropriate business need to use your personal data which does not overly prejudice you

### **46. Additional legal grounds for special categories of personal data:**

- 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.***

47. 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 data with them. Further details on the third parties who may need access to your information is set out in sections below.

**48. 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

**49. Additional legal ground for special categories of personal data:**

- a) I need to use the personal 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

50. 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 the following personal data related to your treatment:

- a) your NHS Number in England and Wales, CHI Number in Scotland or Health and Care Number in Northern Ireland),
- b) the nature of your procedure;
- c) the length of your stay in hospital;
- d) any complications such as infection or the need for an unplanned transfer or readmission/admission to a NHS facility;
- e) any adverse incidents which arose during the course of your treatment;
- f) any revision surgery required;
- g) your recovery and improvement post-treatment; and
- h) the feedback you provided as part of any PROMs surveys.

51. PHIN will use your personal data in order to share it with the NHS, and track whether you have received any follow-up treatment. As I am under a specific legal obligation to share personal data relating to your private care and treatment with PHIN, I do not require your consent to do so.

52. The records that I share may contain personal and medical information about patients, including you. For the avoidance of doubt, I will only share personal data to the extent that its disclosure is specifically required by the law. I will not share the entirety of your clinical record with PHIN, and will only disclose the categories of personal data outlined in the previous paragraph. PHIN, like me, will apply the highest standards of confidentiality to personal data 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 personal data, including its Privacy Notice, is available at [www.phin.org.uk](http://www.phin.org.uk).

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

53. 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 data, 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, and potentially share, your personal data (although only to the extent that it is necessary and relevant to the subject-matter).

**54. Legal grounds:**

- a) The use is necessary in order for us to comply with our legal obligations

**55. Additional legal ground for special categories of personal data:**

- a) I need to use the personal 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

56. 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)***

57. 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.

58. **Legal grounds:**

- a) My having an appropriate business need to use your personal data which does not overly prejudice you

***Purpose 9: Provide marketing information to you (including information about other products and services offered by selected third-party partners) in accordance with preferences you have expressed.***

59. As a provider of private healthcare services, I need to carry out marketing but am mindful of your rights and expectations in that regard. As a result, I will only provide you with marketing which is relevant to my business and only where you have specifically confirmed your consent to do so.

60. **Legal grounds:**

- a) My having an appropriate business need to use your personal data which does not overly prejudice you
- b) You have provided your consent

***Disclosures to third parties:***

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

- a) A doctor, nurse, carer or any other healthcare professional involved in your treatment
- b) Other members of support staff involved in the delivery of your care, like receptionists and porters
- c) Anyone that you ask me to communicate with or provide as an emergency contact, for example your next of kin or carer
- d) NHS organisations, including NHS Resolution, NHS England, Department of Health
- e) Other private sector healthcare providers
- f) Your GP
- g) Your dentist
- h) Other clinicians (including their medical secretaries)
- i) Third parties who assist in the administration of your healthcare, such as insurance companies
- j) Third parties identified as acting legitimately on your behalf in connection with legal proceedings (including potential medico-legal claims)
- k) Private Healthcare Information Network
- l) National and other professional research/audit programmes and registries, as detailed under purpose 4 above
- m) Government bodies, including the Ministry of Defence, the Home Office and HMRC

- n) Our regulators, like the Care Quality Commission, Health Inspectorate Wales and Healthcare Improvement Scotland
- o) The police and other third parties where reasonably necessary for the prevention or detection of crime
- p) Our insurers
- q) Debt collection agencies
- r) Credit referencing agencies
- s) Our third party services providers such as IT suppliers, actuaries, auditors, lawyers, marketing agencies, document management providers and tax advisers
- t) Selected third parties in connection with any sale, transfer or disposal of our business
- u) I may also use your personal data 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.

62. I may communicate with these third parties in a variety of ways including, but not limited to, email, post, fax and telephone.

#### **How long do I keep personal information for?**

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. Medical records will be kept in line with the law and national guidance. In most cases the retention period will be 8 years at minimum, and longer if pertaining to diagnoses of cancer, chronic conditions or the care of obstetric patients. Information on how long records are kept can be found at: <https://digital.nhs.uk/article/1202/Records-Management-Code-of-Practice-for-Health-and-Social-Care-2016>

63. If you would like further information regarding the periods for which your personal data will be stored, please contact me using the details outlined in section 3.

#### **International data transfers**

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

65. 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.

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

67. 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 personal data for other purposes. In the event that it is necessary to do so, we will update this Privacy Notice.

### **Your rights**

68. Under data protection law you have certain rights in relation to the personal data that I hold about you. These include rights to know what personal data 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.

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

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

71. 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 data.

72. 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 data***

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

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

75. 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.

76. 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 data about you. If I do hold personal data about you I usually need to explain to you:
  - i. The purposes for which I use your personal data
  - ii. The types of personal data I hold about you
  - iii. Who your personal data has been or will be shared with, including in particular organisations based outside the EEA.
  - iv. If your personal data 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 data. If that is not possible, the criteria I use to determine how long I hold your personal data for
  - vi. If the personal data I hold about you was not provided by you, details of the source of the personal data
  - 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 data
  - ix. Your right to ask me to restrict how your personal data is used or to object to my use of your personal data
  - 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***

77. I take reasonable steps to ensure that the personal data 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)***

78. 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 at [www.nicklinton.org](http://www.nicklinton.org). 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.

79. In some circumstances, you have the right to request that I delete the personal data I hold about you. However, there are exceptions to this right and in certain circumstances I can refuse to delete the personal data in question. In particular, for example, I do not have to comply with your request if it is necessary to keep your personal data 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***



80. 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 data. In particular, for example, I do not have to comply with your request if it is necessary to keep your personal data 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***

81. In some circumstances, I must transfer personal data 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 object to marketing***

82. You can ask me to stop sending you marketing messages at any time and I must comply with your request. You can do this by contacting me using the details provided at section 3 above.

#### ***The right to withdraw consent***

83. In some cases I may need your consent in order for my use of your personal data to comply with data protection legislation. Where I do this, you have the right to withdraw your consent to further use of your personal data. 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***

84. 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 my legal obligations.

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

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

#### **National Data Opt-Out Programme**

87. NHS Digital introduced a national programme which on 25 May 2018, pursuant to which all patients can log their preferences as to sharing of their personal data. 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 personal data to which you object.

### **Updates to this Privacy Notice**

88. 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.

89. This Privacy Notice was last updated on 5<sup>th</sup> February 2019