Data sharing policy

Introduction

1 This is our Data sharing policy.

2 We are the professional regulator for nurses and midwives in the UK, and nursing associates in England. Our principal functions include setting standards of education, training, conduct and performance and ensuring the maintenance of those standards.

3 We are statutorily required to maintain a register of qualified nurses, midwives and nursing associates and to set standards necessary to be admitted to and remain on the register. Where necessary, we investigate concerns about the fitness to practise of nurses, midwives and nursing associates to ensure the maintenance of our standards.

4 We can share personal data if we consider it necessary to perform our regulatory functions. We have specific powers to disclose any information relating to a registrant's fitness to practise if we consider it to be in the public interest. Where appropriate, we must cooperate with other healthcare regulators, employers and educators. This may involve responding to requests to share information. .

Aims of the policy

5 This policy aims to:

5.1 state our commitment to sharing personal data in a way that complies with data protection legislation;

5.2 to state the responsibilities of everyone working for or on our behalf when deciding whether and how to share personal data;

5.3 to set out in general terms any exemptions from the data protection legislation that are likely to apply when responding to requests to share personal data.

Scope

6 The policy covers two main types of data sharing:

6.1 systematic, routine or large-scale data sharing with third party organisations for an established purpose;

6.2 exceptional, one-off decisions to share data with third party organisations or internally within the NMC.

7 This policy does not cover:

7.1 Disclosures made as part of our normal processes, such as routine correspondence with people as part of our registration or fitness to practise processes. These disclosures should be made in accordance with our legislation and our privacy notices and information handling guidance published on our website.

7.2 Sharing personal data in response to individuals who have made subject access requests (see the *Subject access request policy*) or requests for personal data under the Freedom of Information Act 2000.

7.3 The publication of personal data as part of our registration functions and under fitness to practise processes which is set out in separate publication guidance published on our website.

7.4 Sharing personal data with contractors that process personal data on our behalf or jointly. This type of data sharing is governed by our contractual arrangements with those organisations.

Roles and responsibilities

8 The Data Protection Officer is responsible for offering advice on data sharing, including whether it is necessary or appropriate to undertake a Data Protection Impact Assessment (DPIA).

9 Directors are responsible for authorising any arrangement where we agrees to systematic, routine or large-scale data sharing with a third party organisation and ensuring that those arrangements are reviewed on a regular basis.

10 The Customer information and data requests team is generally responsible for responding to ad hoc requests to share personal data made by third parties and third party organisations.

11 Staff at manager grade or above, or manager equivalent, such as lawyers may make exceptional, one-off decisions to share personal data internally or with a third party organisation.

12 All other staff are responsible for:

12.1 ensuring that they act in accordance with any data sharing arrangements that have been put in place when carrying out systematic, routine or large scale data sharing activities;

12.2 co-operating with and assisting the Customer information and data requests team to respond to ad hoc requests to share personal data;

12.3 promptly escalating to their manager any situation where they consider that an exceptional, one off decision needs to be made to share personal data with a third party organisation or with another department within the organisation.

Policy review

13 We will review this policy every year, or more frequently in the event of any legislative or regulatory changes.

Compliance

14 Everyone working for us or on our behalf is required to understand and comply with this policy.

15 Any alleged breach of this policy may result in an investigation which may result in action being taken by the NMC up to and including dismissal; removal from office; or, termination of a contract for services.

General policy statements

Data sharing and the law

16 Before we share any personal data (on a systematic or ad hoc basis), we will always consider the legal, privacy and governance implications of doing so, including whether:

16.1 we are under a legal obligation to the data;

16.2 there are any specific statutory prohibitions on sharing the data;

16.3 there are any copyright restrictions;

16.4 a duty of confidence is owed or expected which may affect our ability to share the data (for example, medical or banking information);

16.5 there are any potential human rights considerations, such as a possible interference with an individual's right to respect for his private and family life.

17 Staff should seek advice from the Data Protection Officer where the decision to share personal data may be subject to other legal constraints which go beyond the requirements of data protection legislation.

Conditions for processing

18 We will always clearly identify and keep a written record of the purpose or purposes for which we intend to share personal data.

19 We will normally only share personal data where it is:

19.1 necessary to comply with our legal obligations or

19.2 necessary for the performance of a task carried out in the public interest, such as to assist in the prevention, detection or prosecution of crime; or

19.3 necessary for the exercise of official authority vested in the NMC, for example, using our powers under the Nursing and Midwifery Order 2001 to disclose fitness to practise information where it is in the public interest or

19.4 necessary for the purposes of legitimate interests pursued by the NMC and those interests are not overridden by the interests or fundamental rights and freedoms of the data subject; or

19.5 with the explicit consent of the data subject. Given our status as a regulatory organisation (and in light of the concerns set out in the ICO's guidance on consent) any consent must be freely given.

20 We will in general only share special categories of personal data or caution and conviction data where the data subject has given their explicit consent or it is strictly necessary to:

20.1 comply with a legal obligation;

20.2 fulfill our statutory obligations and for reasons of substantial public interest;

20.3 cooperate with other authorities in the detection and investigation of crime or unlawful acts, or the discharge of another regulator's functions.

21 Whenever a decision relates to sharing special category data or cautions and convictions data, we will consider whether or not advice is required from the Data Protection Officer and/or whether a DPIA is required.

Consent

22 We will not rely on (or seek) the data subject's consent where we have decided to share their personal data regardless of their wishes, for example, because we consider it is necessary to comply with a legal obligation or for the performance of a task carried out in the public interest.

23 Even where we do not seek or rely upon consent, we may (depending on the circumstances) consult with the data subject as part of determining whether or not to share their personal data. We will also generally try to inform data subjects where we have decided to share their personal data, unless an exemption applies.

Legitimate interests

24 We will never rely on the "legitimate interests" condition as the legal basis for sharing personal data where:

24.1 the processing would cause unwarranted prejudice to the rights and freedoms or legitimate interests of the data subject

24.2 we are required to share personal data for the performance of a task carried out in the public interest or in the exercise of official authority vested in us.

Fairness and transparency

25 Before we share any personal data with a third party organisation or internally, we must have a clear understanding of how the information will be used by the recipient.

26 We will generally only share personal data where the disclosure of the information would be compatible with the purposes for which we originally obtained it.

27 We will ensure that individuals are fairly informed of the use of their data. We will do this by providing (or making available) fair processing information about our decision to share their personal data.

28 Where we have entered into a systematic, routine or large scale data sharing arrangement, we will provide details of the arrangement to data subjects in our privacy notices which are generally available on our website.

29 Unless an exemption applies, we will normally communicate the following fair processing information to the data subject where we make an exceptional, one-off decision to share personal data:

29.1 who we are;

29.2 why we are going to share their personal data; and

29.3 who we are going to share their personal data with (this could be the actual named organisation or types of organisation) and

29.4 What their data will be used for.

Additional requirements

30 We will only share personal data that is relevant and necessary to the purpose for which the data is shared.

31 We will only share personal data that is, as far as possible, accurate and up-to-date. We will have procedures in place to tell third party organisations that we have shared inaccurate information so that they have the opportunity to correct it. Personal data will be shared in a secure manner in accordance with our *Information classification and handling policy*.

International transfers

32 We may on occasion be required to transfer personal data to countries outside the European Union (EU).

33 As well as complying with the general requirements for sharing data described above, we will put in place additional safeguards when transferring data outside the EU unless we are relying on an exemption..

34 Whenever we decide to transfer data internationally staff must consider seeking advice from the Data Protection Officer. Additionally a record of the decision-making must be kept.

Exemptions

35 The starting point is that we will be fair and explain to data subjects how we intend to share their data. However, there may be circumstances where we may be exempt from certain provisions of the data protection legislation.

36 Where we rely on an exemption we may:

36.1 not provide the data subject with fair processing information when sharing their personal data;

36.2 share personal data with a third party even where the disclosure is incompatible with the purpose for which we originally obtained it; and/or

36.3 not invite the views of the data subject or give particular weight to their views in assessing how to proceed.

37 The circumstances in which we will typically rely on an exemption are:

37.1 because we are required to share the data in question by law (for instance so as to comply with a court order or statutory demand);

37.2 for the prevention or detection of crime, or the apprehension or prosecution of offenders, to the extent that informing the data subject of the disclosure (or complying with various other requirements of data protection legislation) would be likely to prejudice those functions;

37.3 because we are under an obligation to publish the data or otherwise make it available to the public;

37.4 because the disclosure is for the purpose of, or in connection with:

37.4.1 legal proceedings (including prospective legal proceedings);

37.4.2 for the purpose of obtaining legal advice, or

37.4.3 otherwise for the purpose of establishing, exercising or defending legal rights.

to the extent that the above provisions would prevent us from making the disclosure.

38 Where an exemption under the data protection legislation applies, we may decide not to inform the data subject that we have shared their personal data, if telling the data subject would be inconsistent with the purpose of us sharing the information. We may also be exempt from complying with a subject access request or an objection to our processing.

39 A further exemption applies to the provision of fair processing information, subject access, and the right to object to processing to the extent that the processing would be likely to prejudice the proper discharge of our functions or those of another regulator.

40 In some circumstances where an exemption applies we may share personal data with a third party even where the disclosure is incompatible with the purpose for which we originally obtained it.

Specific policy statements

Systematic, routine or large scale data sharing

41 Any new arrangement or service for systematic, routine data sharing with third party organisations must comply with the general policy statements set out above and be authorised by the relevant director before its implementation.

42 We will always carry out a DPIA before any systematic, routine or large scale data sharing takes place between us and another organisation.

43 We will also put in place a Memorandum of Understanding (MoU) and/or data sharing agreement with the other organisation which:

43.1 states the purpose of the data sharing;

43.2 sets out the legal basis on which the data will be processed

43.3 defines which data is to be shared;

43.4 identifies all the organisations that will be involved in the data sharing, including contact details for key members of staff;

43.5 describes how fair processing information will be provided to the data subjects;

43.6 identifies any prohibited uses of the data;

43.7 defines the basis on which the data will be kept secure including during transfer;

43.8 ensures adequate protection for special categories of personal data;

43.9 defines a procedure for the handling of data subject access requests;

43.10 defines for how long the shared data will be retained;

43.11 records what should happen in the event of an incident or complaint involving the data in question.

44 Directors are responsible for ensuring that any MoUs and/or data sharing agreements are reviewed regularly and kept up to date. A central record of our data sharing agreements should be kept by the Data Protection Officer.

Responding to ad hoc requests

45 The Customer information and data requests team is generally responsible for recording and responding to all ad hoc requests for personal data in line with this policy. The exceptions to this is where we receive ad hoc requests to share personal data:

45.1 in the context of a human resources matter. These requests will be dealt with separately by our human resources department.

45.2 from journalists. These requests will be dealt with by the media team.

46 Where a decision to share information could pose a risk to the rights and freedoms of the data subject or our organisation, the decision-maker should seek advice from the Data Protection Officer.

47 In the most sensitive cases, the decision whether or not to agree to the request to share personal data should be escalated to director level and a DPIA must be completed.

48 Before sharing any personal data, the decision-maker must comply with the general policy statements set out above and:

48.1 ensure that there is a written request notice from the organisation seeking the information explaining what information they need, why they need it and what they propose to do with it

48.2 where an exemption from the requirements of data protection legislation is relied upon, a clear explanation is provided by the party seeking disclosure of how the exemption is engaged

48.3 confirm in writing our expectations of how the data should be used by the receiving organisation

48.4 consider whether any non-disclosure arrangements or confidentiality rings need to be put in place, where for example the information being disclosed is sensitive and we wish to control legally how it may be used by the receiving party.

49 Decisions about whether or not to share personal data must be documented and take into account:

49.1 the nature of the request;

49.2 the scale of personal data sought;

49.3 the purposes to which it will be used; and

49.4 the implications for the data subject.

50 If a requestor is not happy with our decision not to disclose personal data they may seek a court order or a statutory demand (where making such a demand is within the powers of the organisation seeking the information).

Requests from law enforcement agencies

51 Where a law enforcement agency is requesting disclosure of information under the crime and taxation exemption, the request:

51.1 must cite the relevant exemptions in the data protection legislation being relied upon to make the request

51.2 must state reasons why the information is required.

52 Other organisations may make requests for information using the law enforcement exemption where they have a crime detection or prosecution function. We will not use any exemptions in respect of civil claims.

53 All exchanges of information between us and the police and other law enforcement agencies and all evidence material originating from the police and other law enforcement agencies are confidential information as defined by our *Information Classification and Handling Policy*.

54 If the law enforcement agency requires that the descriptor 'Private and confidential' should not be used in the email subject line, this should be complied with.

55 When exchanging information with the police and other law enforcement agencies in paper form we must use a special delivery postal service or secure courier. All documents must be securely wrapped in double envelope and must be signed for by the recipient. Any media (such as CDs, DVDs or USB drives) must be encrypted.

Tracer requests

56 We will not generally respond to requests for contact information about a nurse or midwife to enable the enquirer to trace the nurse or midwife. This is because:

56.1 There are no means of authenticating the motive of the person who is making the enquiry about the nurse or midwife in question.

56.2 The nurse or midwife may not wish to be contacted, by the requestor.

56.3 The address we hold for the nurse or midwife may not be current, particularly if they have lapsed and are no longer practising. If the nurse or midwife has moved and we send a letter on behalf of the enquirer a third party (now at the address) may receive personal information about the nurse or midwife.

Proactively sharing data with third party organisations on an ad hoc basis

57 Authorised staff may only share personal data with third party organisations in accordance with this policy.

58 We will in general only proactively share personal data where it is:

58.1 necessary to comply with a legal obligation

58.2 necessary for the performance of a task carried out in the public interest (including the prevention or detection of crime)

58.3 in the exercise of official authority vested in the controller.

59 Where a decision to share personal data could have a significant impact on the data subject or pose a risk to the rights and freedoms of the data subject or our organisation, the decision maker should seek advice from the Data Protection Officer. For example decisions to disclose special category data or data about cautions and convictions.

60 Any decision to share personal data must be documented and set out::

60.1 what data we are sharing

60.2 the purpose of the data sharing

60.3 how the data will be used by the receiving organisation;

60.4 the legal basis on which we are sharing the data

60.5 the name of the organisation we are sharing data with and contact details for key members of staff

60.6 how it is proposed that fair processing information will be provided to the data subjects (unless an exemption applies);

60.7 any prohibited uses of the data;

60.8 the basis on which we are satisfied that the data will be kept secure, including during transfer;

60.9 how special categories of personal data will be adequately protected;

60.10 a procedure for the handling of data subject access requests;

60.11 how long the data we are sharing will be retained by the receiving organisation;

60.12 what should happen in the event of an incident or complaint involving the data in question;

60.13 whether any non-disclosure arrangements or confidentiality rings are to be put in place.

61 The template at Annex 1 should be used to record decisions to share personal data and a copy sent to the Data Protection Officer.

Ad hoc sharing within the NMC

62 We will put in place role-base access controls and other measures to prevent unauthorised internal use of the personal data that we gather.

63 Where managers decide to share information internally (for instance, between directorates), this must comply with the general policy statements above.

64 In addition, managers should only share personal data internally when it would be compatible with the purposes for which we originally obtained it.

65 If it is not, managers shall provide further fair processing information to the data subject to explain how we are intending to use their information and on what legal basis, unless an exemption applies.

66 Where sharing the information could potentially impact on the rights and freedoms of the data subject, a DPIA should be undertaken before deciding to share it.

Glossary

Data controller	A Data controller is a person, public authority, agency or body, which (either alone or jointly or with others) determines the purposes for which and the manner in which any personal data are, or are to be, processed.
Data subject	Any living individual who is the subject of personal data.
Personal data	Any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such an name, an identification number, location data, an online identifier or to one or more factors specific to the physical, psychological, genetic, mental, economic, cultural or social identity of that person. Such personal data might include, but is not be limited to: • Name • Address • Telephone Number • Age • Date of Birth • Qualifications • Education and employment history • A unique reference number
Special Categories of Personal Data (Previously known as "sensitive personal data")	"Special category personal data": comprises information relating to a data subject's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Physical or mental health or condition • Sexual life or sexual orientation • Commission or alleged commission of offences