

Information Sharing Agreement

Between NHS Counter Fraud Authority and The Nursing and Midwifery Council

Date: October 2019

Version control

Version	Name	Date	Comment
V0.1			Review
V1.0		8 July 2019	Final

Parties	4
Purpose and aims	4
Aims	4
Remit of the NHS Counter Fraud Authority	4
Remit of the Nursing and Midwifery Council	5
Information Sharing	5
Single Point of contact	5
Key principles.....	5
Fraud, Corruption or Theft.....	5
Fitness to practise	6
Allegations of criminality.....	6
Decisions to disclose.....	6
Concurrent investigations.....	6
Data items	7
Personal data.....	7
Special Category Data	7
Data Relating to Criminal Convictions and Offences.....	7
Legal basis for sharing	8
NHSCFA statutory function of identifying and tackling fraud across the NHS.....	8
NMC statutory function of protecting the public.....	8
Data Security	8
Access and Individuals rights	9
Freedom of Information requests	9
Subject Access Requests	10
Complaints regarding data	10
Information Governance	10
Audit arrangements.....	10
Ensuring data quality.....	10
Retention of shared data	11
Data Controller	11
Privacy Notices	11
Breach.....	11
Dispute resolution	11
Duration	11
Review	11
Termination	12
Appendix 1	12

Parties

The parties to this information sharing agreement are:

(1) Nursing and Midwifery Council

23 Portland Place, London, W1B 1PZ;

(2) NHS Counter Fraud Authority

Fourth Floor, Skipton House, 80 London Road, London, SE1 6LH; and

(3) NHS Counter Fraud Services (NHS Wales)¹

First Floor Block B, Mamhilad House, Mamhilad Park Estate, Pontypool, NP4 0YP

Purpose and aims

1. The purpose of this Information Sharing Agreement (ISA) is to set out the framework for information sharing between the NHS Counter Fraud Authority (NHSCFA) and the Nursing and Midwifery Council (NMC). It sets down the principles underpinning the interaction between the parties and provides guidance on the exchange of information between them.
2. This ISA does not override the statutory responsibilities and functions of NHSCFA and the NMC and is not enforceable in law. However, NHSCFA and the NMC are committed to working in ways that are consistent with the content of this ISA.

Aims

3. The aims of this ISA are to ensure information is legally and appropriately shared in order to assist the parties to fulfil their statutory functions. In particular to:
 - 3.1 ensure the sharing of information is carried out between the parties in an accurate, adequate, timely and lawful manner;
 - 3.2 promote co-operation between the NMC and the NHSCFA in the conduct of their respective statutory duties;
 - 3.3 facilitate the effective and efficient sharing of information to assist the NMC to protect the public and promote public confidence in the nursing, nursing associate and midwifery professions;
 - 3.4 assist the NHSCFA with information gathering to safeguard NHS resources by assisting with the prevention and detection of fraud and other unlawful activities committed by those working in the NHS.

Remit of the NHS Counter Fraud Authority

4. NHSCFA is an independent Special Health authority. NHSCFA leads on work to identify and tackle fraud across the NHS. Its purpose is to safeguard NHS resources so that the NHS is better equipped to care for the nation's health, providing support, guidance and direction to the NHS. This work enables effective prevention, detection and enforcement action to take place against fraud and fraudulent activity. NHSCFA also collects, collates and analyses information that holds intelligence value, which in turn broadens the understanding of fraud risks in the NHS.
5. NHSCFA has duties and enforcement powers under the NHS Act 2006, the Health and Social Care Act 2012, and the NHS Counter Fraud Authority (Establishment, Constitution and Staff and other Transfer Provisions) Order 2017, issued by the Secretary of State for Health. NHSCFA is responsible for:

¹ NHS Counter Fraud Authority provides NHS anti-fraud services to the Welsh Assembly Government (under section 83 of the Government of Wales Act 2006). For simplicity, the term 'NHS Counter Fraud Authority' is used throughout this document to represent counter fraud services in England (under NHS Counter Fraud Authority) and Wales (under Counter Fraud Services Wales). The signatory for NHS Counter Fraud Authority represents both NHS Counter Fraud Authority (England) and NHS Counter Fraud Services (Wales).

- 5.1 leading on work to protect NHS staff, patients and resources from fraud, bribery and corruption, educating and informing those who work for, who are contracted to, or who use the NHS about fraud in the health service and how to tackle it;
- 5.2 preventing and deterring fraud in the NHS by reducing it and removing opportunities for it to occur or to re-occur; and
- 5.3 holding to account those who have committed fraud against the NHS by detecting and prosecuting offenders and seeking redress where viable.

Remit of the Nursing and Midwifery Council

- 6. The NMC's purpose is to protect the public and promote public confidence in the nursing, midwifery and nursing associate professions. The responsibilities and functions of the NMC are set out primarily in the Nursing and Midwifery Order 2001 and include:
 - 6.1 setting standards of education, training, conduct and performance so that nurses, midwives and nursing associates can deliver high quality healthcare consistently throughout their careers;
 - 6.2 ensuring that nurses, midwives and nursing associates keep their skills and knowledge up to date and uphold their professional standards;
 - 6.3 having fair processes to investigate complaints made against nurses, midwives and nursing associates;
 - 6.5 taking action in response to complaints about nurses, midwives and nursing associates to protect the public.

Information Sharing

Single Point of contact

- 7. The named contacts with responsibility for this ISA are named in Appendix 1. The points of contact will liaise as required to ensure this ISA is kept up to date; identify any emerging issues in the working relationship between the two organisations; and resolve any questions that arise as to the interpretation of this ISA. The points of contact can nominate an appropriate alternative point of contact for day-to-day communication and/or joint working but must communicate this to the other organisation.

Key principles

- 8. Where either the NMC or NHSCFA become aware of matters that appear to fall within the remit of the other organisation, it will, at the earliest opportunity convey the concerns and relevant supporting information to the point of contact in accordance with this ISA.
- 9. Where the parties encounter concerns which come under the sharing remit of this ISA, in the interests of patient safety and protection of the public, the referring organisation will not wait until its own review or investigation has concluded before conveying the concerns.

Fraud and Corruption

- 10. Where NHSCFA receives information or pursues an investigation that a nurse, midwife or nursing associate has been involved in fraud or corruption the NMC will be informed as soon as practicable. The NMC will then be able to consider the matter under its fitness to practise process and whether any further investigation needs to be carried out.
- 11. Where NHSCFA becomes aware of allegations or evidence that an individual may be posing fraudulently as a registered nurse, midwife or nursing associate, either through a stolen identity, fraudulently acquired registration or through falsified qualifications, NHSCFA will immediately contact the NMC via the single point of contact. In these cases, the primary concern for both

parties will be patient safety. The NMC will take whatever action is appropriate in the interests of protecting the public.

12. Where the NMC receives information or investigates the actions of a nurse, midwife or nursing associate which relates to allegations concerning fraud, corruption or theft in the NHS, it will share that information with NHSCFA.

Fitness to practise

13. Where NHSCFA receives information relating to allegations that call into question the fitness to practise of a nurse, midwife or nursing associate, it will share that information with the NMC. Fitness to practise includes the conduct, performance or health of a nurse, midwife or nursing associate. A registrant is 'fit to practise' when they have the skills, knowledge and characters to practise their profession safely and effectively.
14. Further guidance on information relating to referring concerns regarding the fitness to practise of nurse, midwife or nursing associate can be found here: <https://www.nmc.org.uk/concerns-nurses-midwives/dealing-concerns/what-is-fitness-to-practise/>.

Allegations of criminality

15. In cases where there are other allegations of criminality, the NMC will disclose relevant information and documentation to NHSCFA where such allegations are related to fraud or, corruption.
16. Where a case has resulted in a criminal prosecution, NHSCFA will share details of the case with the NMC.
17. In cases where an investigation has concluded that there was no criminal activity, but indicates there may be concerns about the fitness to practise of an NMC registrant, the NHSCFA will pass relevant information to the NMC to enable it to decide on the seriousness of the allegations and whether they should be referred under its fitness to practise process.

Decisions to disclose

18. In cases where the NMC is in doubt as to whether information should be disclosed to NHSCFA, they will make contact with the point of contact specified in Appendix 1 in order to discuss the matter. Any discussions at this stage will be anonymised.
19. In cases where NHSCFA is in doubt as to whether a case should be disclosed to the NMC, they will make contact with the point of contact specified in Appendix 1 in order to discuss the matter. Any discussions at this stage will be anonymised.
20. When information is disclosed by either party, there will be a discussion in advance about the timing of any action, including onward disclosure. Each party will consider any request to delay action which may compromise the other's action, recognising that each party has a responsibility to make decisions in the public interest.
21. If either party shares information under the provisions of this ISA it will provide the other with the necessary information and documentation to permit the other party to investigate, and provide ongoing assistance by providing any additional relevant information and documentation that may reasonably be requested by the other organisation.

Concurrent investigations

22. Where cases have been identified as of mutual interest to NHSCFA and the NMC both parties will endeavour to keep each other informed of findings, actions and updates.

23. There may be occasions when the parties need to undertake concurrent investigations. When this occurs both parties will take steps to ensure that they do not undermine the progress and/or success of each other's investigation. This may include allowing criminal investigations to take place as a priority.

Media Interest

24. Where there is an issue of mutual interest to the parties, the parties will work together to support an anti-fraud culture within the health profession industry and the wider health service.

Data items

24. The parties agree to abide by the Data Sharing Code of Practice produced by the Information Commissioners Office, and recognise their respective responsibilities as public bodies under the General Data Protection Regulation (GDPR), Data Protection Act 2018 (DPA) and the Freedom of Information Act 2000 (FOIA).
25. The GDPR defines the following classes of information relevant to this ISA; 'personal data', 'special categories of data' and 'personal data relating to criminal convictions and offences'.

Personal data

26. Personal data is defined as "any information relating to an identified or identifiable natural person; an identifiable natural person (data subject) is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."
27. The obtaining, handling, use and disclosure of personal data is principally governed by the GDPR, DPA, Article 8 of the Human Rights Act 1998, and the common law duty of confidentiality.
28. The law imposes obligations and restrictions on the way personal data is processed, and the data subject has the right to know who holds their data and how such data will be processed, including how such data will be shared.

Special Category Data

29. Certain types of data are referred to as "special categories of personal data' or 'sensitive personal data". These are data which relate to the data subject's:
- racial or ethnic origin;
 - political opinions;
 - religious or philosophical beliefs;
 - trade union membership;
 - genetic data;
 - biometric data;
 - health;
 - sexual life.
30. Additional and more stringent obligations and restrictions apply whenever sensitive personal data is processed.

Data Relating to Criminal Convictions and Offences

31. There are separate safeguards for personal data relating to criminal convictions and offences, set out in Article 10 of the GDPR. To process personal data regarding convictions or offences there must be a lawful basis under GDPR Article 6 and legal/official authority under Article 10.

Legal basis for sharing

32. The parties are to ensure that the disclosure, access, storage and processing of shared information is accurate, necessary, secure, legal and ethical, taking into account relevant legislation and approved guidance where applicable, including:
- NHS Act 2006;
 - General Data Protection Regulation
 - Human Rights Act 1998;
 - Freedom of Information Act 2000;
 - Data Protection Act 2018;
 - Equality Act 2010;
 - Access to Health Records Act 1990;
 - Computer Misuse Act 1990;
 - Confidentiality: NHS Code of Practice;
 - Common Law Duty of Confidentiality.
33. Information shared between the parties will only be used for their respective statutory purposes; data exchanges will be managed by observing the methods and guidelines outlined in this ISA.
34. When the parties share information they do so in order to perform their respective statutory functions. Each party is solely responsible for determining their legal basis for sharing.

NHSCFA statutory function of identifying and tackling fraud across the NHS

35. The statutory duties and powers of the NHSCFA are set out in the NHS Counter Fraud Authority (Establishment, Constitution and Staff and Other Transfer Provisions) Order 2017². NHSCFA has further duties in the NHS Act 2006, the Health and Social Care Act 2012.
36. Operational work undertaken by NHSCFA is carried out under Article 6, para (e), Article 9(2) paras (f) and/or (g) and Article 10 of the GDPR and Part 3 and Schedule 2 Part 1 of the DPA, for the prevention and detection of crime; under Part 10 of the NHS Act 2006, for the protection of the NHS from fraud and other unlawful activities; and in accordance with the powers contained in part 4 of the NHSCFA (Establishment, Constitution, and Staff and other Transfer Provisions) 2017 and such directions as the Secretary of State for Health may give.

NMC statutory function of protecting the public

37. The statutory duties and powers of the NMC are set out in the Nursing and Midwifery Order 2001³.
38. Under article 3(5)(b)(iv) of the Order, in exercising its functions the NMC shall co-operate in so far as is appropriate and reasonably practicable, with public bodies or other persons concerned with the regulation of health services.
39. Under article 22(10) of the order the NMC may disclose to any person any information relating to a person's fitness to practise which it considers it to be in the public interest to disclose.
40. The NMC will share personal data with NHSCFA under this ISA when the conditions set out in Article 6(1)(f) of the GDPR are met. The NMC will share special category data and personal data relating to criminal convictions and offences when one of the additional conditions set out in Part 2 and/or 3 of Schedule 1 of the DPA is met.

Data Security

41. The NMC and NHSCFA are registered with the Information Commissioner's Office on the Data Protection Register⁴:

² The NHSCFA order can be found at <http://www.legislation.gov.uk/ukxi/2017/958/contents/made>

³ The NMC order can be found at <https://www.nmc.org.uk/globalassets/sitedocuments/legislation/the-nursing-and-midwifery-order-2001-consolidated-text.pdf>

⁴ Registration entries can be found at <http://www.ico.org.uk/esdwebpages/search>, the registration number of the NMC is Z6823359 and the registration number of the NHCFA IS ZA290744

42. As data controllers the parties are expected to treat all information in accordance with the GDPR and the DPA and ensure that security is in place sufficient to protect the information from unauthorised access. This includes physical security, such as adhering to organisational clear desk policies and adequate protection for premises when unattended, to IT related security such as passwords, secure IDs and secure servers.
43. It is understood that the parties may have differing security needs, however it is important that all reasonable steps are made to ensure information is kept secure at all times. Each party is expected to comply with their own Information Security Policy and operating procedures and to make staff aware of their obligations in this respect.
44. Each party's point of contact will ensure that their staff know, understand and will maintain the confidentiality, where appropriate, and security of the information and will ensure that anyone involved with the processing of the information is aware of the penalties of wrongful disclosure.
45. Due to the sensitive nature of operational work carried out by the parties, much of the information held by the parties is of a sensitive nature and is classified by central government as "Official" or 'Official Sensitive'. NHSCFA therefore uses the Public Services Network (PSN) in its operations and in so doing complies with the standard requirements in the code of conduct for Government Connect. The NMC does not subscribe to the government classification.
46. The parties must take appropriate technical and organisational measures against unauthorised or unlawful accessing or processing of information. The parties agree to take steps to prevent accidental loss, destruction or damage of information. This will include:
 - 46.1 appropriate technological security measures, having regard to the state of technology available and the cost of implementing such technology, and the nature of the information being protected;
 - 46.2 secure physical storage and management of non-electronic information;
 - 46.3 password protected computer systems;
 - 46.4 ensuring information is only held for as long as is necessary, in line with data protection obligations; and
 - 46.5 appropriate security on external routes into the organisation, for example internet firewalls and secure dial-in facilities.
47. Access to the information will be restricted to those staff with a warranted business case. Access to information will be via restricted-access password protection and be capable of audit. The means of access to the information (such as passwords) will be kept secure.
48. When the parties share information electronically, it will be in a mutually compatible IT format and shared in a secure method.
49. Where the data to be transferred includes special category data or personal data relating to criminal convictions and offences, one of the following secure methods of transmission will be used:
 - 49.1 encrypted email or file transfer;
 - 49.2 a secure electronic portal;
 - 49.3 encrypted portable media;
 - 49.4 royal mail special delivery service or by courier.

Access and Individuals rights

Freedom of Information requests

- 50 The parties are subject to the Freedom of Information Act 2000 (FOIA). Information relating to NHS business processed by the parties is essentially public sector information; therefore this information

may be subject to Freedom of Information enquiries but only by going through the parties own Freedom of Information process.

- 51 The FOIA provides individuals with a statutory right to access information held by public authorities. Members of the public have a right to be told whether information is held by a public body, and a right to have that information communicated to them, although these rights are subject to certain exemptions. This is called a Freedom of Information Request.
- 52 Requests must be put in writing. Where both parties to this ISA hold the information requested, the organisation who originally held the data will have the responsibility to respond under the terms of FOIA.
- 53 Requests will be considered by the organisation and a decision will be made as to the legality and appropriateness of information disclosure. Any release of information will be in accordance with the law.

Subject Access Requests

- 54 The parties are also subject to the GDPR and DPA. The DPA provides individuals with a statutory right of access (subject to certain exemptions) whereby data subjects can ask to see the information that is held about them (personal data). This is called a Subject Access Request.
- 55 Where both parties to this ISA hold the personal data requested, the organisation who originally held the data will have the responsibility to respond under the terms of the DPA and/or GDPR.
- 56 Requests will be considered by the organisation and a decision will be made as to the legality and appropriateness of information disclosure. Any release of information will be in accordance with the law.

Complaints regarding data

- 57 Complaints from data subjects about personal or sensitive information held by the parties must be made in writing to the person or organisation originally holding the information, detailing the reasons for the complaint. Complaints will then be responded to by the organisation following their official complaints process.

Information Governance

Audit arrangements

- 58 Each party will maintain an information sharing log in respect of the ISA. The log will contain:
 - 58.1 a record of information disclosed to the other party;
 - 58.2 the justification of decisions to disclose or not to disclose;
 - 58.3 a record of the outcome of any referral made and the outcome of the referral;
 - 58.4 an access list recording the authorising officer;
 - 58.5 notes of meetings between the parties;
 - 58.6 a record of any review of the ISA.
- 60 The parties may be required to provide copies of any audits conducted during the period of the ISA, including any audit arrangements or implementation plans.

Ensuring data quality

- 61 The party disclosing data shall ensure that shared data is accurate. Where either party becomes aware of inaccuracies in shared data, they will inform the other party immediately.

Retention of shared data

- 62 Each party shall continue to retain information in accordance with their individual retention and disposal schedules.
- 63 In the absence of a records retention and disposal schedule, or a statutory retention period, the information shall not be retained for longer than is necessary to fulfil the agreed purposes in this ISA.
- 64 The NMC's corporate retention schedule is available on their website at <https://www.nmc.org.uk/contact-us/data-protection/privacy-notice/#retention-schedule>.
- 65 The NHSCFA'S corporate retention schedule is available on their website at:
- Data Handling, Storage, Retention and Records Management Policy

Data Controller

- 66 Under the GDPR, controller means any 'natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.' All data controllers are required to comply with the GDPR when they process personal data.
- 67 Under the framework of this ISA, the parties are each data controllers in their own right. The NMC is a data controller in respect of the organisation's information, and accordingly the NHSCFA is data controller in respect of the information it holds. It is not the intention of either organisation that they will act as joint data controllers at any time of any shared data. When sharing information each organisation will retain distinct legal responsibility for the handling of information that it acquires for the purpose of its statutory functions.

Privacy Notices

- 68 Each party is responsible for providing privacy information to data subjects describing the information that may be used for the purposes outlined in this ISA and their information rights.

Breach

- 69 The parties agree to report promptly breaches of any of the terms of this ISA to the point of contact in Appendix 1 especially breaches of the security of personal data.

Dispute resolution

- 70 Any dispute between the parties will normally be resolved at an operational level. If this is not possible, it may be referred to a Senior Manager who will try to resolve the issues within 14 days of the matter being referred to them.
- 71 Unresolved disputes may be referred upwards through those responsible for operating this ISA up to and including the Chief Executive Officer or Managing Director (or equivalent), who will be jointly responsible for ensuring a mutually satisfactory resolution.

Duration

- 72 This ISA shall commence on the date of its signature by the parties and will remain in effect unless it is terminated, re-negotiated or superseded by a revised document.

Review

- 73 At the end of one year following the commencement of this ISA, it will be formally reviewed by the parties, and will be reviewed again every 12 months. Each annual review will:

- 73.1 report on actions arising from the operation of this ISA within the preceding 12 months;
- 73.2 consider whether this ISA is still useful and fit for purpose, and make amendments where necessary;
- 73.3 refresh operational protocols where necessary;
- 73.4 identify areas for future development of the working arrangements; and
- 73.5 ensure the contact information for each organisation is accurate and up to date.

Termination

- 74 Either party may terminate or re-negotiate this ISA at any time upon giving the other party one month's notice in writing of its intention to do so.
- 75 Upon termination of this ISA each party shall ensure that any data received under this ISA is returned to the original party that held the information or destroyed in the following circumstances:
 - 75.1 on termination of this ISA for whatever reason;
 - 75.2 on expiry of the term (unless extended further to the terms of this ISA);
 - 75.3 once processing of the shared Personal Data is no longer necessary for the purposes it were originally shared for.

Signatories

**Signed for and on behalf of
The Nursing and Midwifery Council**


Signed 

Name Matthew McClelland

Title Director of Fitness to Practise

Date 2 October 2019

**Signed for and on behalf of
NHS Counter Fraud Authority**

Signed 

Name Sue Frith

Title Chief Executive Officer

Date 10th October 2019
