



Medicines & Healthcare products
Regulatory Agency

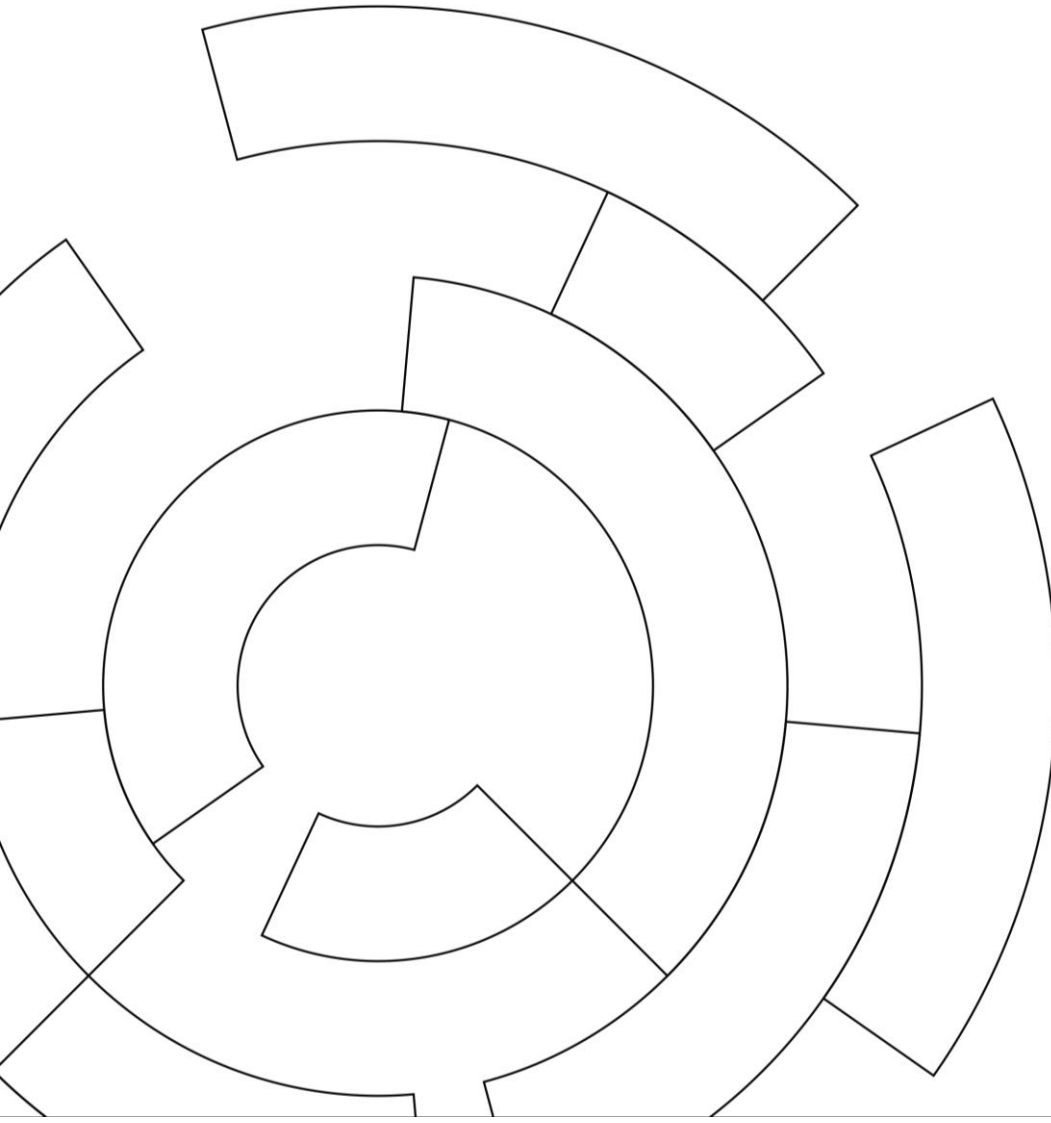


Counter Fraud Authority

Information Sharing Agreement

Between NHS Counter Fraud Authority and the Medicines & Healthcare Products Regulatory Agency.

Date: May 2020



Version control

Version	Name	Date	Comment
V0.1	Helen Moore		
V0.2	Helen Moore	5.4.2020	updated
V0.3	Helen Moore	12.4.2020	updated
V0.4	James Cooke	28.4.2020	updated
V0.5	Helen Moore	30.4.2020	Final version for signature

Between

- (1) **The Medicines and Healthcare products Regulatory Agency (MHRA)**
;and
- (2) **NHS Counter Fraud Authority**
Fourth Floor, Skipton House, 80 London Road, London, SE1 6LH; and
- (3) **NHS Counter Fraud Services (NHS Wales)**
First Floor Block B, Mamhilad House, Mamhilad Park Estate, Pontypool, NP4 0YP¹

being collectively “the Parties”.

Scope and purpose

1. The purpose of the Information Sharing Agreement (ISA) is to set out the framework for information sharing between the NHS Counter Fraud Authority (NHSCFA) and the Medicines & Healthcare Products Regulatory Agency (MHRA). It sets down the principles underpinning the interaction between the parties and provides guidance on the exchange of information between them.

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).

2. Although the Parties agree to adhere to the contents of this agreement, it is not intended to be a legally binding document. The agreement does not override each Party's statutory responsibilities or functions, nor does it infringe the autonomy and accountability of either Party or their governing bodies.
3. The Parties agree to abide by the Data Sharing Code of Practice² produced by the Information Commissioners Office and recognise their respective responsibilities as public bodies under the General Data Protection Regulation 2016, Data Protection Act 2018 and the Freedom of Information Act 2000.

The Aims

4. The aims of this agreement are to:
 - prevent and reduce fraud and corruption within the healthcare profession;
 - maintain service user safety and confidence in the healthcare profession;
 - prevent non-compliance with medicines and medical devices regulations
 - support enforcement of medicines and medical devices regulations
 - support the sharing of information, intelligence, expertise and experience;
 - ensure the sharing of information is carried out between the parties in an accurate, adequate, timely and lawful manner;
 - promote co-operation between NHSCFA and MHRA in the conduct of their respective statutory duties.
5. To facilitate the sharing of information, both Parties will follow due processes as they are defined in the agreement.

Remit of Medicines and Healthcare Products Regulatory Agency

6. The Medicines and Healthcare products Regulatory Agency (MHRA) is an Executive Agency of the Department of Health and Social Care and was established on 1 April 2003. The Agency has three centres:
 - The Clinical Practice Research Datalink (CPRD) - a data research service that aims to improve public health by using anonymised NHS clinical data
 - The National Institute for Biological Standards and Control (NIBSC) - a global leader in the standardisation and control of biological medicines
 - The Medicines and Healthcare products Regulatory Agency (MHRA) regulatory centre - the UK's regulator of medicines, medical devices and blood components for transfusion. The regulatory centre is responsible for: ensuring their safety, quality and efficacy/performance; supporting innovation and new products being developed safely for the benefit of public health; monitoring the safety of medicines devices and blood; and, ensuring secure supply in globalised industries.
7. The MHRA is the UK regulatory authority for medicinal products, medical devices and for blood and blood components.
The MHRA's objectives are to:
 - Safeguard public health through our primary role in ensuring that the products we regulate meet required standards of safety, quality and efficacy;
 - Carry out our communication role through the provision of accurate, timely and authoritative information to healthcare professionals, patients and the public;

² http://www.ico.org.uk/for_organisations/data_protection/topic_guides/data_sharing

- Support research, ensuring through the application of better regulation principles that regulation does not stifle innovation;
 - Influence the shape of the future regulatory framework through use of our effective international relationships; and
 - Run an organisation with a skilled and equipped workforce that is fit for the future.
8. The MHRA is an Executive Agency of the Department of Health and is the UK regulatory authority with responsibility for medicines (for human use) and medical devices and acts as the principle law enforcement agency with responsibility for investigating criminal acts relating to medical products. It enforces the provisions of inter alia:- the Human Medicines Regulations 2012, the Medicines Act 1968, the Blood Safety and Quality Regulations 2005, the Good Laboratory Practice Regulations 1999, the Medicines for Human Use (Transmissible Spongiform Encephalopathies) (Safety) Regulations 2003, and the Medical Devices Regulations 2003.

Remit of NHS Counter Fraud Authority

9. NHSCFA is an independent Special Health Authority established in November 2017. 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
10. NHSCFA has duties and enforcement powers under the NHS Act 2006, the Health and Social Care Act 2012, and the NHSCFA (Establishment, Constitution and Staff and other Transfer Provisions) Order 2017, issued by the Secretary of State for Health. NHSCFA is responsible for:
- 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;
 - preventing and deterring fraud in the NHS by reducing it and removing opportunities for it to occur or to re-occur; and
 - holding to account those who have committed fraud against the NHS by detecting and prosecuting offenders and seeking redress where viable.
11. NHS England follows the NHSCFA strategy when undertaking its own work to tackle fraud,
12. Officers working for NHS England must report any suspicions of economic fraud to NHSCFA as soon as they become aware of them to ensure they are investigated properly and maximise the chances of financial recovery.
13. The majority of allegations of economic fraud will be investigated by Local Counter Fraud Specialists (LCFS) appointed to provide counter fraud services on behalf of NHS England.
14. NHSCFA will work cooperatively with NHS England officers to ensure work is conducted to prevent, deter and detect fraud within and against NHS England.
15. NHSCFA will investigate cases of fraud that cannot be dealt with by NHS England, including cases of bribery and corruption.

Information Sharing

16. The Parties are subject to the duty of confidentiality owed to those who provide them with confidential information and the confidentiality and security of this information will be respected. It is understood by the Parties that statutory and other constraints on the exchange of information will be fully respected, including the requirements of the General Data Protection Regulation 2016, the Data Protection Act 2018, the Freedom of Information Act 2000 and the Human Rights Act 1998.

Intelligence

17. The Parties acknowledge that intelligence can be received by way of complaints, professional whistleblowing, concerns raised by members of the public, referrals from other public bodies (including overseas regulators or investigatory bodies), or by information received from other sources (e.g. from press monitoring or during the course of routine inspections to registered premises).

18. If either Party receives intelligence which:

- indicates a significant risk to the health and wellbeing of the public, particularly in relation to the safety of the healthcare profession or the sale and supply of medicines and / or medical devices
- indicates a significant risk of fraudulent activity against the NHS; and/or
- requires a coordinated multi-agency response;

this information will be shared in confidence with the contact specified in Appendix 1 within the other Party at the earliest possible opportunity.

19. NHSCFA has a responsibility to protect NHS staff, patients and resources from fraud, bribery, and corruption by way of effective prevention, detection and enforcement action against fraudsters and fraudulent activity. To facilitate this work, it is important that intelligence held by MHRA is shared with NHSCFA on a timely basis.
20. To facilitate the work of the MHRA, as specified in paragraph 6 above it is important that intelligence held by NHSCFA is shared with MHRA on a timely basis.

Investigation

21. Where MHRA becomes aware of allegations against people abusing the NHS, NHSCFA will be informed (if it is not clear that they are already aware) if there are clear allegations of fraud, corruption, or bribery.
22. In cases where there are other allegations of dishonesty or criminality, MHRA will disclose relevant information and documentation to NHSCFA where such allegations are relevant to NHSCFA's core functions. However, whether such disclosure takes place will depend on the circumstances of the case and the seriousness of the allegations.
23. In cases where MHRA staff are in doubt as to whether a case should be disclosed to NHSCFA, they will make contact with the point of contact specified below in order to discuss the matter. Any discussions at this stage will be anonymised. MHRA staff will be able to rely on the fact that if the specified NHSCFA contact indicates that they wish to receive full disclosure, this will be on the basis that it is essential for NHSCFA's core purpose or is in the public interest.

24. Where NHSCFA is aware that during or following an investigation, evidence exists that persons of relevance to MHRA have been involved in a breach of medicines or medical devices regulation, MHRA will be informed of such matters. MHRA will consider whether any further investigation needs to be carried out.
25. In cases where NHSCFA staff are in doubt as to whether a case should be disclosed to MHRA, they will make contact with the point of contact specified below in order to discuss the matter. Any discussions at this stage will be anonymised. NHSCFA staff will be able to rely on the fact that if the specified MHRA staff indicate that they wish to receive full disclosure, this will be on the basis that it is essential for MHRA's core purpose or is in the public interest.
26. In cases where an investigation has concluded that there was no fraudulent activity, but indicates there may be concerns about the activities of persons of relevance to MHRA, the information will be passed to MHRA to enable a decision to be taken on the seriousness of the allegations and their relevance to MHRA's core function.
27. When information is disclosed to MHRA there will be a discussion in advance about the timing of any action that MHRA may consider appropriate, including disclosure of the case to the employer and individual involved. MHRA will consider any request to delay action which may compromise any current NHSCFA investigation. However, NHSCFA recognises that action may need to be taken by MHRA where it is in the public interest to do so.
28. Where NHSCFA becomes aware of allegations against people breaching medicines or medical devices regulations MHRA will be informed (if it is not clear that they are already aware).
29. In cases where there are other allegations of dishonesty, criminality or other breaches of medicines/medical devices regulation NHSCFA will disclose relevant information and documentation to MHRA where such allegations are relevant to MHRA's core functions. However, whether such disclosure takes place will depend on the circumstances of the case and the seriousness of the allegations.
30. In cases where NHSCFA staff are in doubt as to whether a case should be disclosed to MHRA, they will make contact with the point of contact specified below in order to discuss the matter. Any discussions at this stage will be anonymised. NHSCFA staff will be able to rely on the fact that if the specified MHRA contact indicates that they wish to receive full disclosure, this will be on the basis that it is essential for MHRA's core purpose or is in the public interest.
31. Where MHRA is aware that during or following an investigation, evidence exists that persons of relevance to NHSCFA have been involved in fraud, corruption or bribery, NHSCFA will be informed of such matters. NHSCFA will consider whether any further investigation needs to be carried out.
32. In cases where MHRA staff are in doubt as to whether a case should be disclosed to NHSCFA, they will make contact with the point of contact specified below in order to discuss the matter. Any discussions at this stage will be anonymised. MHRA staff will be able to rely on the fact that if the specified NHSCFA staff indicate that they wish to receive full disclosure, this will be on the basis that it is essential for NHSCFA's core purpose or is in the public interest.
33. In cases where an investigation has concluded that there was no breach of medicines or medical devices regulation, but indicates there may be concerns about the activities of persons of relevance to NHSCFA, the information will be passed to NHSCFA to enable a decision to be taken on the seriousness of the allegations and their relevance to NHSCFA's core function.
34. When information is disclosed to NHSCFA there will be a discussion in advance about the timing of any action that NHSCFA may consider appropriate, including disclosure of the case to the employer and

individual involved. NHSCFA will consider any request to delay action which may compromise any current MHRA investigation. However, MHRA recognises that action may need to be taken by NHSCFA where it is in the public interest to do so.

35. 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. There may, however, be occasions when MHRA will need to act swiftly to take steps to protect public safety and would do so with due regard for other known ongoing investigations.
36. Where either Party intends to undertake an investigation (over and above any routine inspection activity) the contact in the other Party specified below should be alerted, in confidence, at the earliest possible opportunity.
37. Outcomes arising from any relevant investigations actioned by either Party will be shared with the contact specified in Appendix 2 at the earliest possible opportunity.
38. Where joint or parallel investigations are required, preliminary discussions should resolve any potential areas of conflict or overlap, arising from each Party's respective powers.

Enforcement

39. Where NHSCFA or MHRA has taken or intends to take enforcement action, the outcome of which is relevant to the other Party, details will be shared at the earliest possible opportunity with the single point of contact or the relevant authorised officer in Appendix 2, specified below.

Liaison and dispute resolution

40. The effectiveness of the working relationship between MHRA and NHSCFA will be ensured through regular contact, both formally and informally, at all levels up to and including senior management of the respective Parties.
41. Any dispute between MHRA and NHSCFA will normally be resolved at an operational level. If this is not possible, it may be referred to a Senior Manager on behalf of each Party who will try to resolve the issues within 14 days of the matter being referred to them.
42. Unresolved disputes may be referred upwards through those responsible for operating this agreement, up to and including the Chief Executive Officer or Managing Director (or equivalent) of each Party, who will be jointly responsible for ensuring a mutually satisfactory resolution.
43. The Parties agree to report immediately instances of breaches of any of the terms of this agreement especially of the confidentiality obligations and to raise an appropriate security incident should such a breach occur.

Point of contact

44. The Parties agree to, when possible, share information and intelligence using a single point of contact (SPOC), as specified in Appendix 1. The single point of contact will be responsible for sending and receiving shared information, and will act as facilitator for enquiries (however, this person may not necessarily be the end user or processor of the information).
45. The Parties acknowledge that points of contact within the Parties may differ over time due to the nature of investigative activities and the appropriateness of Party involvement. The Parties may

nominate an appropriate alternative point of contact for day-to-day communication and/or joint-working in the event of an NHSCFA or MHRA investigation taking place which involves a specialised area of business, specialist knowledge or a particular expertise. The nominated person(s) will therefore act as single point of contact for investigation purposes. A single point of contact who understands criminal investigation procedures and what is required to a criminal standard is essential to enable investigators to exchange crucial information in a timely manner, to prevent contradictory information being exchanged, and to ensure delays are minimised.

Types of information

46. The General Data Protection Regulation 2016 essentially defines the following classes of information relevant to this agreement; ‘personal data’, ‘special categories’ and ‘personal data relating to criminal convictions and offences’.
47. The Caldicott Information Governance Review 2013, commissioned by the Department of Health, introduced the term ‘personal confidential data’ across the healthcare system to widen the interpretation of ‘personal data’ and ‘sensitive data’ for patient identifiable information.

Personal data

48. Personal data are 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.’

The obtaining, handling, use and disclosure of personal data is principally governed by the General Data Protection Regulation 2016, Data Protection Act 2018, Article 8 of the Human Rights Act 1998, and the common law duty of confidentiality.

The law imposes obligations and restrictions on the way personal data is processed (in this context processing means any operation or set of operations which is performed on personal data , whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction,) and the data subject has the right to know who holds their data and how such data are or will be processed, including how such data are to be shared.

Special Category Data

49. 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

Additional and more stringent obligations and restrictions apply whenever sensitive personal data is processed.

Data Relating to Criminal Convictions and Offences

50. 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

Personal confidential data

51. In 2013 the Department of Health published the Caldicott Information Governance Review, which was an independent review of how information about patients is shared across the health and care system. The review introduced the term 'personal confidential data' to describe 'personal' and 'sensitive' information about identified or identifiable patients, which should be kept private or secret. The Caldicott Information Governance Review can be found at:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/192572/2900774_InformationGovernance_accv2.pdf

Data controller

52. Under the General Data Protection Regulation 2016, 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 General Data Protection Regulation 2016 whenever they process personal data. At all times, when providing data to partners, the partner responsible for delivering a service will be considered the "data controller",
53. Under the framework of the ISA, the parties are each data controllers in their own right. The MHRA 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 the statutory function.

Information sharing protocol

54. Information disclosed by the Parties will comply with the Government Security Classification System (GSC), In this regard, each piece of information will be assigned a level of protection for its processing. All material with a protective marking will be, where possible, marked at the top and bottom and page numbered, and will have a distribution list. Further information regarding the Government Security Classification System is available in the HM Government Security Policy Framework, which can be found at:

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715778/May-2018_Government-Security-Classifications-2.pdf

55. The level of classification assigned by the Parties to information shared shall be "Official or Official Sensitive" depending on the content.

Most information will fall under the “Official” classification but may need to be further marked to indicate that extra care should be taken when handling the information. If that is the case the marking “Official – Sensitive” should be used. This will be applicable if compromise or loss of the information could have damaging consequences for an individual.

56. The Parties agree that, in relation to information contained in material which is marked as “Official” or ‘Official Sensitive’, that it will not:
- a. disclose, release, communicate, or otherwise make available, the information to any other individual, organisation or third party not directly connected with the work involved without prior agreement and approval of the giving Party, except in the form of non-disclosive statistical data, anonymised data or conclusions;
 - b. use the information for any commercial, industrial or other purpose; or
 - c. copy, adapt, duplicate or otherwise reproduce the information save as provided in this Agreement.
57. If there is a need for the Parties to disclose or supply information to other law enforcement agencies, government departments and agencies, or any specified external body for the purposes of anti-fraud activities, full records will be kept of when and what information is disclosed or supplied to external bodies.

Where disclosure is required by law, the disclosing party will notify the other party, before disclosure. The parties will not make any such disclosure without prior approval by the other party. Disclosures will be made on a case by case basis

Lawful use of information

58. 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 2016
 - Human Rights Act 1998;
 - Freedom of Information Act 2000;
 - Data Protection Act 2018;
 - Equality Act 2010;
 - Medicines for Human Use Regulations 2012
 - Medical Devices Regulations 2002
 - Access to Health Records Act 1990;
 - Computer Misuse Act 1990;
 - Confidentiality: NHS Code of Practice;
 - Common Law Duty of Confidentiality.
59. The Secretary of State for Health has responsibility to make arrangements for healthcare provision nationally and to comply with legislation. The Secretary of State for Health, acting through NHSCFA, has a responsibility to ensure healthcare provision is protected from fraud and other unlawful activities. It is therefore appropriate that information relating to the administration of NHS business may be used for these purposes provided that the requirements of law and policy are satisfied.
60. Information shared between the Parties will only be used for their respective statutory purposes. Data exchanges will be managed by observing the methods and guidance outlined in this ISA.
61. 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

Legal Basis

NHSCFA statutory function of identifying and tackling fraud in the NHS

62. Part 10 of the NHS Act 2006 makes provision for the protection of the NHS from fraud and other unlawful activities. The NHS Act 2006 confers powers upon NHSCFA, as the statutory body responsible for tackling fraud across the NHS, to require the production of information or data from an NHS contractor (defined as any person or organisation providing services of any description under arrangements made with an NHS body) in connection with the exercise of the Secretary of State for Health's counter fraud functions.
63. 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 General Data Protection Regulation 2016 and Part 3 and Schedule 2 Part 1 Section 2(1) and/or Section 5(3) of the Data Protection Act 2018, this allows NHSCFA exemptions from specified obligations in the GDPR, 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 NHS Counter Fraud Authority (Establishment, Constitution, and Staff and other Transfer Provisions) 2017 and such directions as the Secretary of State for Health may give. These can be found at:

NHS Act 2006, Part 10:

<http://www.legislation.gov.uk/ukpga/2006/41/part/10>

General Data Protection Regulation 2016

http://gdpr-legislation.co.uk/Regulations_27_April_2016.pdf

Data Protection Act 2018, Part 3:

<https://www.legislation.gov.uk/ukpga/2018/12/part/3/enacted>

<http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/enacted>

Secretary of State for Health's counter fraud functions:

<http://www.legislation.gov.uk/uksi/2017/958/article/4/made>

64. Information or data shared between MHRA and NHSCFA may be used by the Parties for criminal prosecution purposes if the information or data demonstrates evidence of fraud or other unlawful activities against the NHS and/or the information forms a material part of an investigation.

MHRA function of enforcing medicines and medical devices legislation

65. Regulation 323 Human Medicines Regulations 2012 provides that Secretary of State must enforce or secure the enforcement of the Human Medicines Regulations 2012 in England, Scotland and Wales. The Secretary of State discharges this responsibility by means of the MHRA.
66. Regulation 61 Medical Devices Regulations 2002 and section 12 Consumer Protection Act 1987 provide a legislative regime for the enforcement of medical devices regulation. Relevant enforcement activity is carried out by the MHRA.

67. The MHRA processes data in accordance with the provisions of the Data Protection Act 2018 and related legislation and guidance.

Access and Individuals Rights

Freedom of Information

68. The Parties are subject to the Freedom of Information Act 2000. The principles of the Freedom of Information Act 2000 apply and nothing provided in this Agreement is confidential to the Parties to this Agreement. Information relating to the Parties 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. It is up to the recipient Party to disclose information, or to authorise the disclosure of information, under the terms of the Freedom of Information Act 2000.

69. Under the Freedom of Information Act 2000, individuals can make a request to the Parties for information to be disclosed. This is called a Freedom of Information Request. Requests must be put in writing to the recipient Party following their official Freedom of Information Request process. Requests will be considered by the Party's Information Governance representative and a decision will be made as to the legality and appropriateness of information disclosure.

Subject Access Requests

70. The Parties are subject to the General Data Protection Regulation 2016 and the Data Protection Act 2018. Under the General Data Protection Regulation 2016 and the Data Protection Act 2018, data subjects can ask to see the information that is held on computer and in some paper records about them. This is called a Subject Access Request. If data subjects wish to know what information is held about them, requests must be submitted to the recipient Party following their official Subject Access Request process. Requests will be considered by the Party's Information Governance representative and a decision will be made as to the legality and appropriateness of information disclosure.

Complaints

71. Complaints from data subjects about personal or sensitive information held by the Parties must be made in writing to the person or organisation holding the information, detailing the reasons for the complaint. Complaints must be put in writing to the relevant person or organisation following their official complaints process.

Security of information

72. The MHRA and NHSCFA are registered with the Information Commissioner's Office on the Data Protection Register. Registration entry can be found at:

<http://www.ico.org.uk/esdwebpages/search>

MHRA
NHS Counter Fraud Authority

Registration number: **Z5571792**
Registration number: **ZA290744**

73. Regardless of the type of information being accessed, processed and stored, security is considered of paramount importance. All information held by the Parties are held on secure servers, with access restricted to internal use by appropriately authorised members of staff. As data controllers for the information they collect, the Parties are expected to treat all information in accordance with

the General Data Protection Regulation 2016 and the Data Protection Act 2018 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.

74. 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 private and confidential 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. As administrators of NHS business, the Parties are also expected to comply with the standard requirements in the NHS Code of Practice for Information Security Management and the NHS Information Governance Guidance on Legal and Professional Obligations, which can be found at:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/200506/Information_Security_Management_-_NHS_Code_of_Practice.pdf

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/200702/NHS_Information_Governance_Guidance_on_Legal_and_Professional_Obligations.pdf

75. Each Party's responsible officer will ensure that their staff know, understand and guarantee to maintain the confidentiality 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.
76. 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. MHRA complies with the information security regime that it is subject to by, inter alia, using the GOV network.
77. The Parties must take appropriate technical and organisational measures against unauthorised or unlawful accessing and/or processing of information and against accidental loss or destruction of, or damage to, information. This will include:
- 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;
 - secure physical storage and management of non-electronic information;
 - password protected computer systems;
 - ensuring information is only held for as long as is necessary, in line with data protection obligations; and
 - appropriate security on external routes into the organisation, for example internet firewalls and secure dial-in facilities.
78. Each Party is responsible for its own compliance with security in respect of the General Data Protection Regulation 2016 and Data Protection Act 2018, irrespective of the specific terms of this Agreement.
79. The physical and technical security of the information will be maintained at all times. Where the Parties share information electronically, it will be in a mutually compatible IT format and shared in a pre-determined secure method.

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:

- encrypted email or file transfer
 - a secure electronic portal
 - encrypted portable method
 - Royal Mail special delivery service or by courier
80. 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.
81. Laptops used to access information must be encrypted and secured to an HM Government approved or recognised level, commensurate with the level of the protective marking of the information involved as will any network they are connected to.
82. The Parties may be required to provide copies of any audits conducted during the period of the Agreement, including any audit arrangements or implementation plans.

Retention of information

83. Information shall be stored in accordance with the Parties' records retention and disposal schedule.

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 specified purpose or purposes.

Breach and Dispute Procedures

84. The Parties agree to report immediately instances of breaches to any of the terms of this Agreement and to raise an appropriate security incident.

Any disputes arising between the giving and receiving Parties will be resolved initially between the principles of this Agreement. Otherwise, outstanding issues will be referred to an executive group established on behalf of each party.

Audit Arrangements

85. The Parties will maintain an information sharing log in respect of the agreement.

The log will contain:

- A record of the NHSCFA information disclosed;
- A record of MHRA information disclosed;
- A record of information received;
- The decision of justification to disclose or not to disclose;
- An access list recording the authorising officer;
- Notes of meetings with partners;
- A record of any review of the agreement.


Duration and review

86. This agreement shall commence on the date of its signature by the Parties and will remain in effect for a term of one year unless it is terminated, re-negotiated or superseded by a revised document.
87. At the end of one year following the commencement of the agreement, the agreement will be formally reviewed by the Parties, and will be reviewed again no less frequently than on each anniversary of its signing. Each annual review will:
- report on actions arising from the operation of this agreement within the preceding 12 months;
 - consider whether the agreement is still useful and fit for purpose, and make amendments where necessary;
 - refresh operational protocols where necessary;
 - identify areas for future development of the working arrangements; and
 - ensure the contact information for each organisation is accurate and up to date.
88. Following each annual review, the agreement shall automatically renew for a further period of one year, unless terminated or re-negotiated by either Party.
89. Either Party may terminate or re-negotiate this agreement at any time upon giving the other Party one month's notice in writing of its intention to do so.
90. This agreement is not legally binding and is not intended to create legal relationships between the Parties.

Signatories

91. The duly authorised signatories of the Parties to this agreement have executed this agreement as of the date set out below:

Signed for and on behalf of Medicines and Healthcare products Regulatory Agency	
Signed	
Name	Andy Morling
Title	Head of Enforcement
Date	12 May 2020

Signed for and on behalf of NHS Counter Fraud Authority	
Signed	
Name	Sue Frith
Title	Chief Executive Officer
Date	12 May 2020

This Agreement is made on the 12th of May 2020.