



# MEMORANDUM OF UNDERSTANDING

between

Health and Care Professions Council

and

NHS Scotland Counter Fraud Services

DRAFT

## Between

- (1) **Health and Care Professions Council**  
Park House, 184 Kennington Park Road, London, SE11 4BU; and
- (2) **NHS Scotland Counter Fraud Services**  
3 Bain Square, Livingston, EH54 7DQ

being collectively “the Parties”.

## Scope and purpose

1. This Memorandum of Understanding (MOU) describes the roles of the Health and Care Professions Council (HCPC) and NHS Scotland Counter Fraud Services (CFS) and outlines the basis of cooperation and collaboration between the two Parties. It sets down the principles underpinning the interaction between the two Parties and provides guidance on the exchange of information between them.
2. This MOU is a statement of principle; more detailed operational protocols and guidance may be developed, as and when these are required.
3. This MOU applies to Scotland and is intended to provide a framework to assist the joint working of the Parties to ensure maximum effectiveness and efficiency when carrying out investigations. The MOU includes practical arrangements designed to ensure the relationship is effective and that together both Parties meet their aims and objectives, particularly when there are overlapping interests and responsibilities.
4. Although the Parties agree to adhere to the contents of this MOU, it is not intended to be a legally binding document. The MOU 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.
5. Both Parties agree to abide by the Data Sharing Code of Practice<sup>1</sup> produced by the Information Commissioners Office, and recognise their respective responsibilities as public bodies under the Data Protection Act 1998 and the Freedom of Information Act 2000.
6. The aims of this MOU are to:
  - reduce fraud, corruption and theft within the health and care professions to an absolute minimum;
  - maintain service user safety and confidence in the health and care professions;
  - support the sharing of information, intelligence, expertise and experience;
  - contribute to improving the regulatory oversight of the health and care professions; and
  - define the circumstances in which the two organisations will act independently.
7. The term “information” is used in this MOU by CFS to refer to any and all information or data used for NHS Scotland business purposes and by the HCPC to refer to any and all information used for its regulatory functions, including commercial, business, personal and sensitive information or data. The medium in which information or data may be displayed, presented, shared, disclosed or processed, may be in the form of hard-copy or electronic data, records or documents.
8. To facilitate the sharing of information, both Parties will follow due processes as they are defined in the Information Sharing Agreement at **Annex 1**.

## Health and Care Professions Council

<sup>1</sup> [http://www.ico.org.uk/for\\_organisations/data\\_protection/topic\\_guides/data\\_sharing](http://www.ico.org.uk/for_organisations/data_protection/topic_guides/data_sharing)

9. The HCPC is the independent statutory regulator of the 16 professions set out below. The HCPC's main objective in exercising its functions is to safeguard the health and well-being of persons using or needing the services of its registrants.
10. The responsibilities and functions of the HCPC are set out in the Health and Social Work Professions Order 2001 (The Order). The Order protects one or more designated titles set out below for each of the relevant professions, and anyone using one of those titles must be registered with the HCPC. Misuse of a title is a criminal offence.

<b>Profession</b>	<b>Protected titles</b>
Arts therapist	<ul style="list-style-type: none"> <li>• Art psychotherapist</li> <li>• Art therapist</li> <li>• Drama therapist</li> <li>• Music therapist</li> </ul>
Biomedical scientist	<ul style="list-style-type: none"> <li>• Biomedical scientist</li> </ul>
Chiropodist / podiatrist	<ul style="list-style-type: none"> <li>• Chiropodist</li> <li>• Podiatrist</li> </ul>
Clinical scientist	<ul style="list-style-type: none"> <li>• Clinical scientist</li> </ul>
Dietitian	<ul style="list-style-type: none"> <li>• Dietitian</li> <li>• Dietician</li> </ul>
Hearing aid dispenser	<ul style="list-style-type: none"> <li>• Hearing aid dispenser</li> </ul>
Occupational therapist	<ul style="list-style-type: none"> <li>• Occupational therapist</li> </ul>
Operating department practitioner	<ul style="list-style-type: none"> <li>• Operating department practitioner</li> </ul>
Orthoptist	<ul style="list-style-type: none"> <li>• Orthoptist</li> </ul>
Paramedic	<ul style="list-style-type: none"> <li>• Paramedic</li> </ul>
Physiotherapist	<ul style="list-style-type: none"> <li>• Physiotherapist</li> <li>• Physical therapist</li> </ul>
Practitioner psychologist	<ul style="list-style-type: none"> <li>• Practitioner psychologist</li> <li>• Registered psychologist</li> <li>• Clinical psychologist</li> <li>• Counselling psychologist</li> <li>• Educational psychologist</li> <li>• Forensic psychologist</li> <li>• Health psychologist</li> <li>• Occupational psychologist</li> <li>• Sport and exercise psychologist</li> </ul>
Prosthetist / orthotist	<ul style="list-style-type: none"> <li>• Prosthetist</li> <li>• Orthotist</li> </ul>

Radiographer	<ul style="list-style-type: none"> <li>• Radiographer</li> <li>• Diagnostic radiographer</li> <li>• Therapeutic radiographer</li> </ul>
Social workers in England	<ul style="list-style-type: none"> <li>• Social worker</li> </ul>
Speech and language therapist	<ul style="list-style-type: none"> <li>• Speech and language therapist</li> <li>• Speech therapist</li> </ul>

11. Under The Order the principal functions of the HCPC are to establish standards of education, training, conduct and performance of members of the relevant professions and to ensure the maintenance of those standards. It does this by:

- setting standards, including Standards of Proficiency, Standards of Conduct, Performance and Ethics and Standards of Education and Training;
- approving education programmes and qualifications which meets its standards,
- maintaining a register of appropriately qualified professionals; and
- investigating and adjudicating concerns about fitness to practise.

### NHS Scotland Counter Fraud Services (CFS)

12. NHS Scotland Counter Fraud Services (CFS) was established in July 2000.

13. CFS leads on work to protect NHS Scotland resources from financial crime. CFS provides support, guidance and direction to NHS Scotland, enabling effective deterrence, prevention, detection and investigation to take place against criminals and financial crime activity. It also manages improved financial crime intelligence and information flows across the health service.

14. In order to provide an agile, flexible and effective response to the threat of financial crime within and against NHS Scotland, CFS focuses on four key principles.

- DETER – by raising awareness of the impact of financial crime and of the sanctions applied to those who commit such offences against NHS Scotland. This can take place through communications and promotion such as awareness campaigns and media management.
- DISABLE – by improving NHS Scotland’s long term capability to prevent financial crime. This will be achieved by removing or reducing the opportunities for financial crime to occur or recur and by ensuring robust systems are in place.
- DETECT – by improving knowledge sharing and intelligence about financial crime, enhanced data analysis and a proactive approach to countering financial crime.
- DEAL WITH – by investigating the most serious and harmful threats and seeking to apply all relevant sanctions.

## Principles

15. The HCPC's role in regulating health and care professionals means that its processes are distinct from those of the NHS.
16. The HCPC is committed to working collaboratively with CFS, the NHS as a whole, and others, to ensure that service user and the public's safety is upheld. This MOU is intended to ensure that effective channels of communication are maintained between the Parties.
17. CFS is committed to fighting fraud, corruption, theft and other financial irregularities within the NHS in Scotland. Working in collaboration with the HCPC will ensure service users and the public are protected and allegations of suspected fraud, corruption or theft, which are received by the HCPC, can be passed to CFS for investigation. Such information is vital for CFS to ensure that systems and procedures can be assessed for their ability to prevent, reduce, detect or measure fraud, corruption and theft within the NHS in Scotland.

## Working together

18. Fraud, corruption and theft within the NHS are unacceptable. Fraud, corruption and theft divert essential NHS funds and resources away from service user care and, where health and care professionals are involved in such offences, undermines service users' confidence and trust in those professions.
19. It is in the interests of service users that effective action is taken against the small minority of health and care professionals who are engaged in fraud, corruption or theft and, to that end, the HCPC and CFS will cooperate to tackle fraud, corruption and theft within the health service.
20. The HCPC and CFS intend that their working relationship will be characterised by the development of this MOU, through which both parties can:
  - reduce fraud, corruption and theft within the health service to an absolute minimum;
  - make decisions that promote service user and public safety;
  - share information, intelligence, expertise and experience;
  - address overlaps and gaps in the regulatory framework;
  - cooperate openly and transparently with the other Party;
  - respect each Party's independent status; and
  - use resources effectively and efficiently.

## Commitments

21. As signatories to this MOU, both Parties agree to a joint professional approach in support of the following commitments:
  - Supporting a real anti-crime culture within the health service, where fraud, corruption and theft are regarded by everyone as unacceptable and where everyone understands the role they can play in eliminating such offences.
  - Support and where possible facilitate initiatives to ensure that fraud, corruption and theft can be measured accurately.
  - Support initiatives to revise policies, procedures and systems, so as to minimise the risk of fraud, corruption and theft being perpetrated and to ensure that, where necessary, they clearly distinguish between deliberate crime and unintentional error.
  - Ensure, through compliance with suitable guidance, that all cases of suspected fraud, corruption or theft are examined in a fair, objective, expert and professional way, to demonstrate the truth

or otherwise of the suspicion, and that where fraud, corruption or theft is proved press for appropriate sanctions to be imposed.

- In recognition of the reality that it is only through access to information that the truth or otherwise of a suspicion of fraud, corruption or theft can be determined, cooperate in sharing ways of accessing information where this is in the public interest.
- Work together to ensure that CFS's anti-fraud anti-corruption anti-theft strategy is effective and this MOU remains meaningful, relevant and subject to review.

## Information

22. Both Parties hold and use sensitive information about organisations and individuals in order to perform their core functions. It is important that such information is on occasion shared between the Parties. The Parties recognise that this exchange of information needs to be carried out responsibly and within the guidelines set out in this MOU.
23. Both 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 both Parties that statutory and other constraints on the exchange of information will be fully respected, including the requirements of the Data Protection Act 1998, the Freedom of Information Act 2000 and the Human Rights Act 1998.
24. Both Parties are committed to the principle of "collect once, use many times", as a means to reducing the burden of administration and regulation.
25. Where it supports the effective delivery of their respective roles and responsibilities, and the aims of this MOU, both Parties agree:
  - to develop mechanisms to systematically and routinely share the types and categories of data (metadata) that they collect and hold; and
  - to work towards systematically and routinely sharing identifiable data within those categories.
26. The HCPC routinely publishes information about the sanctions it has imposed when registrants are not fit to practise.

## Intelligence

27. Both 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 healthcare premises).
28. If either Party receives intelligence which:
  - indicates a significant risk to the health and wellbeing of the public, particularly in relation to the conduct of a HCPC registrant;
  - indicates a significant risk of criminal activity against the NHS; and/or
  - requires a coordinated multi-agency response;

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

29. CFS has a responsibility to protect NHS staff, patients and resources from crime, including fraud, bribery, corruption, theft and other financial irregularities. To facilitate this work, it is important that

intelligence held by the HCPC relating to HCPC registrants' fitness to practise is shared with CFS in a timely manner.

30. The HCPC is responsible for regulating health and care professionals, which includes taking action when allegations are received which question a registrant's fitness to practise. This can include allegations relating to fraudulent activity. To facilitate this work, it is important that intelligence held by CFS relating to investigations into health and care professionals is shared with the HCPC in a timely manner.

## Investigation

31. Where the HCPC becomes aware of allegations relating to fraud, corruption, theft or other financial irregularity against a registrant working in or for the NHS in Scotland the matter will be reported to CFS as soon as possible in order to ensure it is investigated appropriately and to maximise the chances of financial recovery.
32. Reports to CFS can be made via the Crimestoppers hotline on [08000 15 16 28](tel:08000151628) or by completing an online form at [www.cfs.scot.nhs.uk](http://www.cfs.scot.nhs.uk). The latter method is encouraged as this will enable the HCPC, as a health and care regulatory body, to create an online account for reporting allegations of fraud, corruption or theft in the NHS in Scotland. By having an account, the HCPC will be able to report matters quickly and more efficiently as and when they arise, and will be able to monitor progress of reports made.
33. In cases where there are other allegations of dishonesty or criminality, the HCPC will disclose relevant information and documentation to CFS where such allegations are relevant to CFS's core functions. However, whether such disclosure takes place will depend on the circumstances of the case and the seriousness of the allegations.
34. In cases where the HCPC is in doubt as to whether a case should be disclosed to CFS, 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. The HCPC will be able to rely on the fact that if the specified CFS contact indicates that they wish to receive full disclosure, this will be on the basis that it is essential for CFS's core purpose or is in the public interest.
35. Where CFS is aware that during or following an investigation, evidence exists that a HCPC registrant has been involved in fraud, corruption, theft or any financial irregularity the HCPC will be informed of such matters. The HCPC will then consider whether the concerns meet its Standard of Acceptance for allegations for investigation under its fitness to practise process.
36. In cases where CFS is in doubt as to whether a case should be disclosed to the HCPC, 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. CFS will be able to rely on the fact that if the specified HCPC contact indicates that they wish to receive full disclosure, this will be on the basis that that is essential for the HCPC's core purpose or is in the public interest.
37. Where a case has resulted in a criminal prosecution, CFS will share details of the case with the HCPC. That information will already be in the public domain and consent to disclose that information will not be required.
38. In cases where an investigation has concluded that there was no criminal activity, but indicates there may be concerns about the activities of a HCPC registrant the information will be passed to the HCPC to enable it to decide whether the concerns meet its Standard of Acceptance for allegations for investigation under its fitness to practise process. The HCPC will share that information with the HCPC registrant and their representatives and other third parties involved in the case (where appropriate)

and through the provision of that information to the HCPC, CFS is consenting to the disclosure of that information.

39. When information is disclosed to the HCPC there will be a discussion in advance about the timing of any action that the HCPC may consider appropriate, including disclosure of the case to the HCPC registrant and employer involved. The HCPC will consider any request to delay action which may compromise any current CFS investigation. However, CFS recognises that action may need to be taken by the HCPC where it is in the public interest to do so.
40. In cases where CFS becomes aware of allegations or evidence that an individual may be posing as a HCPC registrant, either through a stolen identity, fraudulently acquired registration or through falsified qualifications, CFS will immediately contact the HCPC via the point of contact specified below. CFS will provide all available information that might suggest that an individual is posing as a HCPC registrant. In these cases, the primary concern for both Parties will be service user safety. The HCPC will take whatever action is appropriate in the interests of protecting service users.
41. 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 the HCPC will need to act swiftly to take steps to protect public safety and would do so with due regard for other known ongoing investigations.
42. Where either Party intends to undertake an investigation the contact in the other Party specified below should be alerted, in confidence, at the earliest possible opportunity.
43. Outcomes arising from any relevant investigations actioned by either Party will be shared with the contact specified below at the earliest possible opportunity.
44. 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

45. Where CFS has taken or intends to take enforcement action or the HCPC intends to take action, the outcome of which is relevant to the other Party, details will be shared at the earliest possible opportunity with the contact specified below.

## Communication

46. Areas of communication between the Parties include, but are not limited to:
  - **sharing of expertise and experience**  
Meetings as and when required between Managers within the Fitness to Practise and Registration departments of the HCPC and counterparts within CFS to facilitate the development of effective investigative methodologies. These meetings may involve discussion about particular cases (anonymised if appropriate) and the Parties may be able to share information about approaches to investigations which have been successful in particular circumstances or about useful contacts within other organisations.
  - **discussions about strategy/policy**  
Meetings as and when required between the Parties will provide an opportunity to discuss strategic/policy developments which may impact on each other's work. Whilst it is not possible to predict all future developments which may be of mutual interest, it is clear that when either Party is reviewing disclosure policies, for example, discussion will be valuable.



- **discussions about individual registrants**

Whilst both Parties have very distinct roles, it is clear that there is an overlap where there are allegations that a registrant working in or for the NHS in Scotland has acted dishonestly or fraudulently and one or both Parties are investigating the individuals in question. Where this kind of issue arises, it is essential that knowledge and information is shared at an early stage between the two Parties in order to allow both to carry out their core functions.

- **sharing experiences of investigations or trends**

From the many cases that both Parties handle, common themes frequently arise. Working collaboratively and sharing this information will enable trends and weaknesses to be quickly identified. Opportunities to deal with the cause of the problems can be discussed and wherever possible fed into policy discussions to work towards changes in practice to prevent further opportunities for fraud, corruption, theft and other dishonesty.

- **sharing views and information about how improved performance might be encouraged**

By sharing this information, appropriate strategies for disseminating information on best practice can be identified and implemented.

- **publicising joint working commitments**

Making known the Parties' commitment to working together to support an anti-crime culture within the health service, including where possible promotion of the NHS Fraud and Corruption Reporting Line.

47. The working relationship between the Parties will be characterised by regular ongoing contact and the open exchange of information and intelligence, through both formal and informal meetings at all levels, including senior levels.
48. Disclosures from either Party to the other will be regularly monitored to ensure that arrangements are working effectively. To facilitate the sharing of information and intelligence, both Parties will follow due processes as they are defined in the Information Sharing Agreement at **Annex 1**.

### Liaison and dispute resolution

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

### Point of contact

53. The Parties agree to, when possible, share information and intelligence using a single point of contact (SPOC). The SPOC 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).

54. Both Parties acknowledge that points of contact within either Party may differ over time due to the nature of investigative activities and the appropriateness of Party involvement. Both Parties may nominate an appropriate alternative point of contact for day-to-day communication and/or joint-working in the event of a CFS 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.
55. For both Parties, the preferred method of information transfer for general enquiries, general communications and small data attachments (for example, Microsoft or PDF files not exceeding 15 MB) will be by email. Attachments must be password protected and where possible compressed within a zipped folder (compression decreases the size of files and reduces the space they use in computer systems). Passwords will be disclosed separately upon receipt of the information.
56. For both Parties, the preferred method of information transfer for large volume information sharing (such as downloads of complete datasets where size exceeds 15 MB), will be by saving the information to a removable media device (for example, a USB stick, pen drive or CD) and dispatching the removable media device to the receiving Party, either by hand delivery, Royal Mail Special Delivery or by a courier service. The removable media device must be encrypted to approved standards to protect the information and the information itself must be password protected. Un-encryption processes and passwords will be disclosed separately upon receipt of the removable media device and the information it contains.
57. The single point of contact for the HCPC (who will have responsibility for nominating an appropriate alternative point of contact for day-to-day communication and/or joint-working in the event of an CFS investigation) will be:

Name	Kelly Holder (September 2016 – December 2016)
Title	Director of Fitness to Practise
Address	Health and Care Professions Council, Park House, 184 Kennington Park Road, London, SE11 4BU
Phone	020 7840 9125
Email	<a href="mailto:kelly.holder@hcpc-uk.org">kelly.holder@hcpc-uk.org</a>

Name	John Barwick (January 2017 – March 2018)
Title	Acting Director of Fitness to Practise
Address	Health and Care Professions Council, Park House, 184 Kennington Park Road, London, SE11 4BU
Phone	020 7840 9109
Email	<a href="mailto:John.barwick@hcpc-uk.org">John.barwick@hcpc-uk.org</a>

58. The single point of contact for CFS (who will have responsibility for nominating an appropriate alternative point of contact for day-to-day communication and/or joint-working in the event of an CFS investigation) will be:

Name	Gordon Young
Title	Head of Counter Fraud Services
Address	NHS Scotland Counter Fraud Services, 3 Bain Square, Livingston, EH54 7DQ
Phone	01506 705237
Email	gordon.young2@nhs.net

**Duration and review**

59. This MOU 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.

60. At the end of one year following the commencement of the MOU, the MOU will be formally reviewed by both 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 MOU within the preceding 12 months;
- review the effectiveness of this MOU in achieving its aims, 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.

61. Following each annual review, the MOU shall automatically renew for a further period of one year, unless terminated or re-negotiated by either Party.


62. Either Party may terminate or re-negotiate this MOU at any time upon giving the other Party one month’s notice in writing of its intention to do so.

63. This MOU is not legally binding and is not intended to create legal relationships between the Parties.

**Signatories**

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

<b>Signed for and on behalf of</b>	
<b>Health and Care Professions Council</b>	
Signed	
Name	Marc Seale
Title	Chief Executive and Registrar

<b>Signed for and on behalf of</b>	
<b>NHS Scotland Counter Fraud Services</b>	
Signed	
Name	Gordon Young
Title	Head of Counter Fraud Services

Date 29 / 09 / 2016

Date 29 / 09 / 2016

65. This MOU is made on the 29 of September 2016.

DRAFT

# Information Sharing Agreement

## Purpose of agreement

66. The aim of this Agreement is to define how information or data may be shared between the Parties and the methods used by the Parties for the secure and legal management, accessing, storage and processing of that information or data.
67. The purpose of this Agreement is to:
- set out the operational arrangements for the exchange of information or data between the Parties; and
  - set out the principles and commitments the Parties will adopt when they collect, store and disclose information or data.
68. The terms “information” or “data” is used in this Agreement to refer to any and all information or data used for CFS’s or the HCPC’s purposes, including commercial, business, personal and sensitive information or data. The medium in which information or data may be displayed, presented, shared, disclosed or processed, may be in the form of hard-copy or electronic data, records or documents.

## Types of information

69. The Data Protection Act 1998 essentially defines three types of information, which are ‘anonymised and aggregated data’, ‘personal data’ and ‘sensitive data’, the latter two relating to living persons. 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’ to include deceased persons.
70. Whilst the Data Protection Act 1998 has defined these three types of information, some information within these areas will have different levels of responsibility and risk associated with them.

### Anonymised and aggregated data

Anonymised data are individual data records from which the personally identifiable fields have been removed. Aggregated data are data which are processed to produce a generalised result, and from which individuals cannot be identified.

### Personal data

Personal data are defined as ‘...data which relate to a living individual who can be identified a) from those data, or b) from those data and other information which is in the possession of, or is likely to come into the possession of, the information provider or information consumer, and includes any expression of opinion about the individual and any indication of the intentions of the information controller or any other person in respect of the individual.’

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

Such personal data might include, but not be limited to:

- name;
- address;
- date of birth;
- telephone number;
- case history;
- a unique reference number if that number can be linked to other information which identifies the data subject.

The law imposes obligations and restrictions on the way personal data is processed (in this context processing includes collecting, storing, amending and disclosing data), and the individual who is the subject of the data (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.

### **Sensitive data**

Certain types of data are referred to as "sensitive personal data". These are data which relate to the data subject's:

- racial or ethnic origin;
- political opinions;
- religious beliefs, or other beliefs of a similar nature;
- trade union membership;
- physical or mental health or condition;
- sexual life;
- commission or alleged commission of any offence;
- any proceedings for any offence committed, or alleged to have been committed.

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

### **Personal confidential data**

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 individuals, which should be kept private or secret, and includes deceased as well as living people. This affords protection under information governance processes to personally identifiable information relating to deceased persons, as such data is outside the scope of the Data Protection Act 1998. The Caldicott Information Governance Review can be found at:

[https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/192572/2900774\\_InfoGovernance\\_accv2.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/192572/2900774_InfoGovernance_accv2.pdf)

The term 'personal confidential data' describes personal and sensitive information relating to identified or identifiable individuals, whether living or deceased. For the purposes of this MOU, 'personal' includes the Data Protection Act 1998 definition of personal data, but it is adapted to include deceased as well as living people and 'confidential' includes both information 'given in confidence' and 'that which is owed a duty of confidence' and is adapted to include 'sensitive' data as defined in the Data Protection Act 1998.

## Data control

71. Under the Data Protection Act 1998, any organisation which “determines the purposes for which and manner in which any personal data are, or are to be, processed” is called a “data controller”. All data controllers are required to comply with the Data Protection Act 1998 whenever they process personal data (bearing in mind, that “processing” includes collecting, storing, amending and disclosing data). At all times, when providing data to partners, the partner responsible for delivering a service will be considered the “data controller”, as opposed to the partner who may be the first point of contact. Partner organisations which receive data from that responsible delivery authority are considered to be “data processors” i.e., processing those data “on behalf of” the delivery partner. As a data processor, partners must at all times process data solely in accordance with the specified instructions and security obligations set out in this Agreement.

## Sharing framework

72. The Parties agree and acknowledge that they each collect and store information.
73. The Parties agree to share information with each other in order to assist with the performance of their statutory functions.
74. When the giving Party discloses information to the receiving Party, that information shall be disclosed for the purposes of the performance of the Parties’ statutory functions.
75. Where the giving Party shares information with the receiving Party, it may share the information in a manner it considers appropriate, although the receiving Party may from time to time make recommendations to the giving Party as to the most practicable means by which information may be shared. If the Parties wish to share information electronically, it will be in a mutually compatible IT format and shared in a secure method. The preferred methods of information transfer are set out on page 11 of the MOU.
76. In relation to the sharing of information, each of the Parties shall take all measures necessary to ensure their respective compliance with all relevant legislation, including, but not limited to, regulations or restrictions regarding disclosure of information to third parties. Each Party will be responsible for processing information in accordance with all applicable data privacy and related regulations (data protection obligations). In particular, information held by either Party will not be kept for longer than provided for under the data protection obligations, and will be destroyed in an appropriate manner conforming to the data protection obligations when no longer required.
77. The information provided by the giving Party shall be accessed by authorised personnel within the receiving Party. Both protectively marked material and non-protectively marked material (see below), whether in hard-copy or electronic format, held by either Party, will be stored securely.
78. If there is a need for either Party to disclose or supply information to law enforcement agencies, government departments and agencies, or any specified external body for the purposes of anti-crime activities, full records will be kept of when and what information is disclosed or supplied to external bodies.

## Lawful use of information

79. In writing this Agreement due attention has been paid to the views of both Parties where possible, and all guidance has been written to ensure that the disclosure, access, storage and processing of shared information is accurate, necessary, secure, legal and ethical, taking into account relevant legislation where applicable.

80. Information or data shared between the HCPC and CFS may be used by either Party 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.
81. Both 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 either Party to this Agreement. Information relating to NHS Scotland business processed by either Party is essentially public sector information; therefore this information may be subject to Freedom of Information enquiries but only by going through either Party's 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. Public sector information which is subject to the provisions of the Freedom of Information Act 2000 cannot be accessed under Freedom of Information processes by going directly to a third party data processor.
82. Under the Freedom of Information Act 2000, individuals can make a request to either Party 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.
83. Both Parties are subject to the Data Protection Act 1998. Under the Data Protection Act 1998, 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 put in writing 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.
84. Complaints from data subjects about personal or sensitive information held by either Party 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

85. The HCPC and CFS 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>

Health and Care Professions Council    Registration number: **Z6621691**  
National Services Scotland                      Registration number: **Z5801192**

86. Regardless of the type of information being accessed, processed and stored, security is considered of paramount importance. All information held by both 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, both Parties are expected to treat all information in accordance with the Data Protection Act 1998, 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.



87. It is understood that each Party 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.
88. Each Party's Information Governance representative 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.
89. Due to the sensitive nature of operational work carried out by CFS, much of the information held by both Parties is of a sensitive nature and is classified by central government as "Official - Restricted".
90. Both 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.
91. Each Party is responsible for its own compliance with security in respect of the Data Protection Act 1998, irrespective of the specific terms of this Agreement.
92. The physical and technical security of the information will be maintained at all times. No disclosable information will be sent by fax or email (unless protected) and, if posted, will be encrypted to approved standards to protect the information and dispatched by Royal Mail Special Delivery service or by courier.
93. For both Parties, 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.
94. 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.
95. Both Parties reserve the right to request details of their information security processes, procedures and certifications to provide assurance that information covered by the agreement is handled and stored securely in accordance with the terms of the agreement.