MEMORANDUM OF UNDERSTANDING

between

HM Revenue and Customs
Risk and Intelligence Service
Gateway Exchange Team

and

NHS Protect (England) and
NHS Counter Fraud Services (Wales)

The Parties

(1) **HM Revenue and Customs**
Gateway Exchange Team, CEI Cardiff, Ty-Glas Road, Llanishen, Cardiff, CF14 5TS; and

(2) **NHS Protect (NHS England)**
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 0YP

NHS Protect 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 Protect' is used throughout this document to represent counter fraud services in England (under NHS Protect) and Wales (under Counter Fraud Services Wales). The signatory for NHS Protect represents both NHS Protect (England) and NHS Counter Fraud Services (Wales).

Purpose of MOU

1. This Memorandum of Understanding (MOU) sets out the arrangements and obligations between Her Majesty's Revenue and Customs (HMRC) and NHS Protect (on behalf of England and Wales), governing the exchange and sharing of information. It should be noted that 'exchange' covers all transfers of information between the two organisations, including where one organisation has direct access to information or systems in the other.

2. The aim of this MOU is to define and facilitate how information may be shared between the Parties and the methods, principles and procedures used by the Parties for the secure and legal management, accessing, storage, processing and retention of that information and the responsibilities each Party owes in respect of the other.

3. The purpose of this MOU is to:

   - set out the operational arrangements for the exchange of information between the Parties; and
   - set out the principles and commitments the Parties will adopt when they collect, store and use information.

4. This MOU sets out the nature and extent of the information to be shared; and the purpose and identity of the information consumer and the information provider. Both Parties may be an information consumer and information provider in relation to this MOU.

5. Information will only be exchanged where it is lawful to do so. The relevant legal bases are detailed within this MOU.

6. The term 'information' is used in this MOU to refer to any and all information or data used for business 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.

7. Information 'consumer' means the Party who receives information. Information 'provider' means the Party who provides information. Information 'controller' means the Party who determines the purposes for which any personal information are to be processed. Information 'processor', in

relation to personal information, means the Party who processes the information on behalf of the information 'controller'.

8. This MOU is not a contract nor is it legally binding. It does not in itself create lawful means for the exchange of information; it simply documents the processes and procedures agreed between the Parties. The MOU should not be interpreted as removing or reducing existing legal obligations or responsibilities on each Party, for example as data controllers under the Data Protection Act.

HM Revenue and Customs

9. Her Majesty's Revenue and Customs (HMRC) is the UK's tax authority. HMRC is responsible for making sure that the money is available to fund the UK's public services and for helping families and individuals with targeted financial support.

10. Further information on HMRC is available at:

www.hmrc.gov.uk

NHS Protect

11. NHS Protect is the operating name of the NHS Counter Fraud and Security Management Service, which is part of the NHS Business Services Authority. NHS Protect was established in September 1998 by an order made by the Secretary of State for Health (SI 2002/3039) pursuant to powers granted by the National Health Service Act 1977.

12. NHS Protect leads on work to identify and tackle crime across the NHS, and to protect NHS staff and resources from crime. It has national responsibility for tackling:

- fraud, bribery and corruption;
- violence, harassment and abuse;
- theft and criminal damage; and
- other unlawful action such as market-fixing.

These are all activities that would otherwise undermine the effectiveness of the health service and its ability to meet the needs of patients and professionals.

13. NHS Protect's objective is to establish a safe and secure environment within the health service both for service users and service providers that has systems and policies in place to: protect people from violence, harassment and abuse; safeguard personal property from theft or criminal damage; and protect NHS assets, equipment, buildings and other resources from misuse so that the NHS is better equipped to care for the nation's health.

14. NHS Protect protects NHS staff, patients and resources by providing support, guidance and direction to NHS health bodies via a network of Local Counter Fraud Specialists (LCFS) and Local Security Management Specialists (LSMS). This work enables effective prevention, detection and enforcement action to take place against criminals and criminal activity. NHS Protect also manages improved criminal intelligence and information flows across the health service.

15. NHS Protect's work covers three main objectives:

- to educate and inform those who work for or use the NHS about crime in the health service and how to tackle it;

- to prevent and deter crime in the NHS by removing opportunities for it to occur or to re-occur; and
- to hold to account those who have committed crime against the NHS by detecting and prosecuting offenders and seeking redress where viable.

16. NHS Protect also provides NHS anti fraud services to the Welsh Assembly Government (under section 83 of the Government of Wales Act 2006) as well as leading on:

- NHS counter terrorism security preparedness;
- national data analysis and risk assessment; and
- anti fraud and pro-security research.

17. Further information can be found at:

http://www.nhsbsa.nhs.uk/3349.aspx
http://www.wales.nhs.uk/sitesplus/955/page/63057

Working together

18. The Parties agree to lawfully and appropriately share information for the purposes of exercising their statutory and public functions.

19. Further details of the purpose(s) for the sharing of information, and specific measures and controls relating to the sharing of information for those purposes, are included within this MOU.

Types of information

20. 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.

21. 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

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

22. 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 MOU.

Sharing framework

23. The Parties agree and acknowledge that they each collect and store information. Where the Parties decide to share information with each other, it will share that information according to the information sharing protocols described within this MOU and with due regard to the anti fraud requirements in the NHS Standard Contract, which can be found at:

    http://www.england.nhs.uk/wp-content/uploads/2013/03/contract-gen-conds.pdf

24. When the information provider discloses information to the information consumer, that information shall be disclosed for the purposes of the prevention, detection, investigation and prosecution of crime or any other unlawful activity, and where failure to disclose would be likely to prejudice those objectives.

25. Disclosure of information will only be made in relation to identified cases, and any decision to disclose will be made on a case by case basis.

26. Any request for information whose purpose is the prevention, detection, investigation and prosecution of crime or any other unlawful activity should specify as clearly as possible how failure to disclose would prejudice the stated objective. The request should make clear:

    - why it is envisaged that the provision of the information would prevent crime; and or
    - why apprehension or prosecution of an offender e.g. why proceedings might fail without the information is necessary to detect a criminal offence or will assist in the information.

27. Sensitive information relating specifically to an identifiable person's medical/clinical records cannot be disclosed unless: express written permission from the data subject is obtained; there are explicit legal vires permitting its disclosure; or it is by order of the Courts.

28. Where the information provider shares information with the information consumer, it may share the information in any manner it considers appropriate, although the information consumer may from time to time make recommendations to the information provider as to the most practicable means by which information may be shared.

29. If the Parties wish to share information electronically, it will be in a mutually compatible IT format and shared in a secure method.

30. 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.

31. Information disclosed by the information provider shall be accessed only by authorised personnel within the information consumer. Both protectively marked material and non-protectively marked material, whether in hard-copy or electronic format, held by either Party, will be stored securely.

Lawful use of information

32. In writing this MOU 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. Both Parties agree to comply with all legal requirements, as well as the common law duty of confidentiality, relating to the disclosure, access, storage and processing of information (particularly personal information), taking into account relevant legislation where applicable, including but not limited to:

- Freedom of Information Act 2000;
- Data Protection Act 1998;
- Human Rights Act 1998;

33. HMRC is bound by a statutory duty of confidentiality which is set out in legislation at Section 18 (1) of the Commissioners for Revenue and Customs Act 2005 (CRCA). This is underpinned by a criminal offence of wrongful disclosure of information that identifies a person (legal or natural) or enables their identity to be deduced, which is set out at Section 19 of the CRCA. Under sections 18 (2) and (3) of the CRCA there are a number of exceptions to the duty of confidentiality that enable lawful disclosure. These include a disclosure which is made:

- for the purposes of a function of the Revenue and Customs and which does not contravene any restriction imposed by the Commissioners (S 18 (2) (a));
- in the public interest in the specific circumstances set out in legislation at S 20 CRCA (S 18 (2) (b));
- in response to a Court Order that is binding on the Crown (S 18 (2) (e));
- with the consent of each person to whom the information relates (S 18 (2) (h);
- through any other enactment, i.e. a statutory information sharing gateway (S 18 (3)).

34. HMRC may disclose information to NHS Protect using the legal gateway in section 19 of the Anti Terrorism, Crime and Security Act 2001 (ATCSA). This allows HMRC to disclose information to another law enforcement agency for the purposes of assisting criminal investigations or proceedings, including for the purpose of determining whether investigations or proceedings should be initiated or brought to an end. All disclosures must comply with the Anti Terrorism Crime and Security Act 2001: Code of Practice on the Disclosure of Information (COP) and must be proportionate. The Code of Practice can be found at:

http://www.hmrc.gov.uk/pdfs/cop_at.htm

35. 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 NHS Protect, has a responsibility to ensure healthcare provision is protected from crime and other unlawful activities. It is therefore appropriate that information pertinent to an NHS investigation may be obtained and used for these purposes provided that the requirements of law and policy are satisfied.

36. Information shared between the Parties must be relevant to an investigation and should only be used for the lawful purpose specified in the request and shall not be further processed in any manner incompatible with that purpose. Use of shared information will comply with the NHS Business Services Authority information security policy and operating procedures, which can be found at:

http://www.nhsbsa.nhs.uk/Documents/NHSBSACorporatePoliciesandProcedures/Information_Security_Policy.pdf

37. 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 NHS Protect, as the statutory body responsible for tackling crime across the NHS, to require the production of information 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.

38. Operational work undertaken by NHS Protect is carried out under Section 29 of the Data Protection Act 1998, 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 such directions as the Secretary of State for Health may give.

39. The disclosure of information to NHS Protect will be actioned within a legal framework, as permitted under Part 10 of the NHS Act 2006 and Section 29 of the Data Protection Act 1998, and in connection with the exercise of the Secretary of State for Health's counter fraud functions. These can be found at:

- NHS Act 2006, Part 10:
  http://www.legislation.gov.uk/ukpga/2006/41/part/10

- Data Protection Act 1998, Section 29:
  http://www.legislation.gov.uk/ukpga/1998/29/section/29

- Secretary of State for Health's counter fraud functions:
  http://www.nhsbsa.nhs.uk/Documents/Sect_1_-_B1_BSA_Directions_2013.pdf

40. Information supplied to NHS Protect may be used by NHS Protect for criminal investigation and prosecution purposes if the information demonstrates evidence of crime or other unlawful activities against the NHS and/or the information forms a material part of an investigation.

41. NHS Protect may disclose information to HMRC using the crime exemption at section 29 (3) of the Data Protection Act 1998. This allows NHS Protect to disclose personal data when it is for the prevention and detection of crime, the apprehension or prosecution of offenders, or for the assessment or collection of any tax or duty or of any imposition of a similar nature.

42. NHS Protect agrees to comply with all legal requirements, as well as the common law duty of confidentiality, relating to the disclosure, access, storage and processing of any sensitive personal

confidential information), taking into account relevant legislation where applicable, including but not limited to:

- Health and Social Care Act 2012;
- Health and Social Care Act 2008;
- NHS Act 2006;
- Human Rights Act 1998;
- Disability Discrimination Act 1995;
- Access to Health Records Act 1990;
- Computer Misuse Act 1990;
- Confidentiality: NHS Code of Practice;
- Common Law Duty of Confidentiality.

Protective marking

43. Information disclosed by either Party will comply with the Government Security Classification System (GSC), which has three markings: "Top Secret", "Secret" and "Official". In this regard, each piece of information will be assigned an appropriate level of protection for its handling, processing, storage and movement. 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 and the Government Security Classifications documents, which can be found at:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/200552/HMG_Security_Policy_Framework_v10_0_Apr-2013.pdf

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/251480/Government-Security-Classifications-April-2014.pdf

44. It is anticipated that the levels of protection assigned by both Parties to information shared shall be "Official" or "Secret" depending on the content.

Official

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.

Secret

Very sensitive information that justifies heightened protective measures to defend against determined and highly capable threats should be marked as "Secret". For example, where compromise could seriously damage the investigation of very serious organised crime. The threat profile for "Secret" anticipates the need to defend against a higher level of capability than would be typical for the "Official" level. This includes sophisticated, well resourced and determined threats, such as highly capable serious organised crime groups.

45. Both Parties agree that, in relation to information contained in material which is marked as "Official" or "Secret", 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 information provider, 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 MOU.

46. If there is a requirement for either Party to disclose or supply shared information to other law enforcement agencies, government departments and agencies, or any specified external body for the purposes of anti crime activities, this will be done in conjunction with the information provider and full records will be kept of when and what information is disclosed or supplied to external bodies.

Point of contact

47. The Parties agree to, where possible, share information using a single point of contact (SPOC). 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).

48. Both Parties may nominate an appropriate alternative point of contact for day-to-day communication and/or joint-working in the event of an investigation taking place which involves a specialised area of business, specialist knowledge or a particular expertise. The nominated person will therefore act as single point of contact for investigation purposes. A single point of contact who understands 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.

49. 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. Key contacts are included in **Annex 3** and **Annex 4**. Each Party will keep the other informed about any changes in the details of key contacts**.**

Procedure for HMRC to obtain data from NHS Protect

50. Every request for disclosure of information must be made in writing (hard copy, secure e-mail or fax). A specimen request form is at **Annex 1**. Requests made other than in writing will not normally be accepted.

51. Disclosures will be made on a case-by-case basis. Requests must therefore be for a specifically named individual. Bulk requests and lists will not be accepted.

52. The request must contain details of the criminal investigation or criminal proceedings to which it relates and specify the information required.

53. Any HMRC officer may make a request but it must be submitted to NHS Protect via the HMRC SPOC, within the Gateway Exchange Team (GET), as listed in **Annex 3**:

cri.gatewaydisclosure@hmrc.gsi.gov.uk

54. Authorisation is to be given only if the authorising officer is satisfied that the request is for the purpose of obtaining information to assist the HMRC enquiry.

55. HMRC authorising officers must be of Senior Officer grade or above.

56. HMRC will keep NHS Protect informed about any changes in the details of the contacts listed in **Annex 3**.

57. A request should bear the appropriate level of protective marking under the Government Security Classification System. In this regard, each piece of information will be assigned an appropriate level of protection for its handling, processing, storage and movement. 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.

58. Requests may be sent by post or email to:

    Information and Intelligence Unit
    NHS Protect
    Fourth Floor Skipton House
    80 London Road
    London
    SE1 6LH

    ciu@nhsprotect.gsi.gov.uk

59. For postal requests, where the contents are deemed "Official" under the Government Security Classification System, these should be double enveloped (e.g. the inner envelope should be marked "Official" or higher and sealed inside another envelope without a security marking on it and show a return address in the event of non-delivery). The protective marking must be shown prominently on the inner cover only.

60. E-mail requests using the Government Secure Intranet (GSI) address should only be up to "Official" under the Government Security Classification System and include the authorisation from the authorising officer in the e-mail chain.

61. NHS Protect will consider and, if satisfied that the request is for the purposes of a criminal investigation/prosecution, will normally disclose the requested information to the full extent that NHS Protect holds that information. The disclosure will always be proportionate to the purpose for which it was sought.

62. Any disclosure by NHS Protect will be made in writing or by secure electronic communication to the SPOC or requesting officer or the officer who authorised and transmitted the request.

63. Spontaneous disclosures by NHS Protect to HMRC are to be made in 5x5x5 format preferably to:

    intelligence.bureau@hmrc.gsi.gov.uk

64. If necessary contacting the HMRC Intelligence Bureau on 03000 521 779 for advice.

Procedures for NHS Protect to obtain data from HMRC

65. Every request for disclosure of information must be made in writing (by e-mail, preferably) on the latest Gateway Exchange Team template available through the GET SPOC whose details are at **Annex 3**. A request made other than in writing will be accepted only in very exceptional circumstances.

66. Disclosures will be made on a case-by-case basis. Requests must therefore be for a specifically named individual or company. Bulk requests and lists will not be accepted.

67. The request must contain details of the criminal investigation or criminal proceedings to which it relates and specify the information required, e.g. current address, or details of income for a stated year.

68. Any NHS Protect officer, or Local Counter Fraud Specialist (LCFS) working on behalf of an NHS health body, may make a request but it must be submitted to HMRC via one of the NHS Protect contacts listed in **Annex 4**, who cannot self-authorise. Authorisation is to be given only if the authorising officer is satisfied that the request is for the purpose of obtaining information to assist in a criminal investigation and/or prosecution.

69. NHS Protect authorising officers must be of a Band 8 grade or above.

70. NHS Protect will keep HMRC informed about any changes in the details of the contacts listed in **Annex 4**.

71. A request should bear the appropriate level of protective marking under the Government Security Classification System. In this regard, each piece of information will be assigned an appropriate level of protection for its handling, processing, storage and movement. 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.

72. Requests may be sent by post or preferably by email to:

GET Cardiff
Room G72 HMRC
Gateway Exchange Team
CEI Cardiff
Ty-Glas Road
Llanishen
Cardiff
CF14 5TS

cri.gatewaydisclosure@hmrc.gsi.gov.uk

73. Exceptional postal requests should be double enveloped (e.g. the inner envelope should be marked “Official” and sealed inside another envelope without a security marking on it and show a return address in the event of non-delivery). The protective marking must be shown prominently on the inner cover only.

74. E-mail requests using the Government Secure Intranet (GSI) address should only be up to “Official” under the Government Security Classification System and include the authorisation from the authorising officer in the e-mail chain.

75. Providing that the principles of the Code of Practice have been respected and the HMRC Gateway Exchange Team (GET) is satisfied that the request is for the purposes of a criminal investigation and/or prosecution, it will normally disclose the requested information to the full extent that HMRC holds that information. The disclosure will always be proportionate to the purpose for which it was sought.

76. Any disclosure by HMRC will be made in writing or by secure electronic communication to the single point of contact (SPOC) or requesting officer or the officer who authorised and transmitted the request. Where the contents of the disclosure are deemed "Official" under the Government Security Classification System, these should be double enveloped in all postal communication (e.g. the inner envelope should be marked "Official" or higher and sealed inside another envelope without a security marking on it and show a return address in the event of non-delivery). The protective marking must be shown prominently on the inner cover only.

77. Spontaneous disclosures by HMRC to NHS Protect are to be made to:

ciu@nhsprotect.gsi.gov.uk

Responsibilities under the Data Protection Act 1998 and the Human Rights Act 1998

78. Both organisations are legally obliged to handle personal information according to the requirements of the Data Protection Act 1998, the Human Rights Act 1998 and the Freedom of Information Act 2000. The principles of each Act apply and nothing provided in this MOU is confidential to either Party to this MOU.

79. HMRC and NHS Protect are public authorities for the purposes of section 6 of the Human Rights Act 1998. It is unlawful for HMRC and NHS Protect to act in a manner that is incompatible with the European Convention on Human Rights.

80. HMRC and NHS Protect undertake to comply with the requirements of the Data Protection Act 1998 and the Human Rights Act 1998 in carrying out any of the actions described in this MOU.

81. HMRC is the data controller of any information it processes for the purposes of its functions where that information comprises personal data or sensitive personal data as defined in sections 1 (1) (personal data) and 2 (sensitive personal data) of the Data Protection Act 1998, including any information it acquires from NHS Protect for the purposes of HMRC's functions under the procedures set out in this MOU.

82. NHS Protect is the data controller of any information it processes for the purposes of its functions where that information comprises personal data or sensitive personal data as defined in sections 1 (1) (personal data) and 2 (sensitive personal data) of the Data Protection Act 1998, including any information it acquires from HMRC for the purposes of NHS Protect functions under the procedures set out in this MOU.

Requests under the Data Protection Act 1998 and the Freedom of Information Act 2000

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 Party processing the information following their official subject access request process.

84. Both Parties are subject to the Freedom of Information Act 2000. 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 respective Party following their official freedom of information request process.

85. If either Party receives a request for information under the Freedom of Information Act 2000 involving information which originated from the other, the Party receiving the request will liaise

with the Freedom of Information Manager (or equivalent) for the originator of the information to determine whether the originator wishes to claim an exemption under the provisions of the Freedom of Information Act 2000. The Party receiving the request must be mindful of the timeframe for response.

86. If either Party receives a subject access request for personal data under section 7 of the Data Protection Act 1998 involving personal data which it is processing but which originated from the other, in accordance with paragraphs 51 and 52 it will action that request in accordance with statutory requirements and timeframes, liaising with the Freedom of Information Manager (or equivalent) for the originator of that personal data as to disclosure and as to any applicable exemptions.

87. Complaints from data subjects about personal or sensitive information held by either Party, or disputes about freedom of information requests, must be made in writing to the Freedom of Information Manager (or equivalent) of the organisation holding the information, following their official complaints process, detailing the reasons for the complaint.

88. Subject access requests, freedom of information requests and/or complaints about either of these will be considered by the recipient Party's Information Governance Manager (or equivalent) and a decision will be made as to the legality and appropriateness of information disclosure.

89. Freedom of Information contacts are listed in **Annex 3** and **Annex 4**.

Information quality

90. Both Parties have a duty of care towards the information being shared. The information provider shall ensure the information it provides is of sufficient quality, namely:

- adequate;
- relevant;
- accurate; and
- not excessive in relation to the purposes for which it is required.

91. Information discovered to be inaccurate or inadequate for its required purpose will be notified to the information provider as soon as is practicable. The information provider will be responsible for correcting the information and notifying the information consumer and all other recipients of the information, who must also ensure that the correction is made.

Information security

92. Both HMRC and NHS Protect 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

HMRC	Registration number: **Z9034158**
NHS Protect	Registration number: **Z9395747**

93. 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.

94. 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.

95. NHS Protect is 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:

http://systems.hscic.gov.uk/infogov/codes/securitycode.pdf

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

96. Each Party's Information Governance Manager (or equivalent) 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.

97. Due to the sensitive nature of operational work carried out by NHS Protect, much of the information held by NHS Protect is of a sensitive nature and is classified by the Government Security Classification System as "Official - Sensitive". NHS Protect therefore uses the Government Secure Intranet (GSI) network in its operations and in so doing complies with the standard requirements in the code of conduct for Government Connect.

98. 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.

99. 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 MOU.

100. The physical and technical security of the information will be maintained at all times. No sensitive information will be sent by fax or email (unless security marked to the appropriate level and protected) and, if posted, will be security marked and protected to approved standards to protect the information and dispatched by Royal Mail Special Delivery service or by courier.

101. 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.

102. 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.

103. Both Parties reserve the right to conduct an audit of confidentiality and security procedures and practices for guaranteeing the security and confidentiality of the information covered by this MOU.

104. Both Parties may be required to provide copies of any audits conducted during the period of the MOU, including any audit arrangements or implementation plans.

Information transfer

105. For both Parties, the preferred method of information transfer for general enquiries, general communications and small data attachments not containing confidential personal information (for example, Microsoft or PDF files not exceeding 15 MB) will be by email (via the Government Secure Intranet (GSI) network). 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.

106. 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 secure file transfer, using either FTPS or SFTP, whereby files can be transferred from one host to another over a Transmission Control Protocol (TCP) network, such as the internet. Files must be encrypted and password protected to approved standards to protect the information. De-encryption processes and passwords will be disclosed separately upon receipt of the information.

107. For all information transfers, an appropriate level of protective security marking will be applied to the information being transferred.

Information handling assurances

108. Both Parties will be provided with only the information necessary and proportionate to meet the business objective specified in the request.

109. Both Parties will not disclose information supplied by the information provider to any outside organisation unless permitted or required by law and not outside the EEA, and will not make any such disclosure without prior approval by the information provider.

110. The information exchange process has been risk assessed by the HMRC Data Guardian Team who provide data security advice to the Risk and Intelligence Service Directorate within which the Gateway Exchange Team (GET) is managed.

111. Both Parties agree to:

- only use the information for purposes that are in accordance with the legal basis under which they received it;
- only hold the information while there is a business need to keep it;
- ensure that only people who have a genuine business need to see the information which it receives will have access to it;

- store information received securely and in accordance with the prevailing central government standards, for example in secure premises and on secure IT systems;
- move, process and destroy information securely, i.e. in line with HM Government Security Policy Framework, issued by the Cabinet Office, when handling, transferring, storing, accessing or destroying information;
- comply with reporting requirements (e.g. reporting information losses or wrongful disclosure), in line with the Cabinet Office Checklist for Managing Potential Loss of Data or Information;
- report any data losses, wrongful disclosures or breaches of security to the designated contact listed in **Annex 3** or **Annex 4** immediately (within 24 hours of first discovering the possibility of a data loss or wrongful disclosure). This includes both advising and consulting with the other Party on the appropriate steps to take, e.g. notification of the Information Commissioner's Office or dissemination of any information to the data subjects; and
- allow the other Party, if required, to carry out an audit to help in deciding whether information should continue to be provided upon request.

112. Each Party will provide an annual report or a report on request, which has been complied with these undertakings by submitting a written report detailing the arrangements and management controls that are in place to protect the confidentiality of information provided by either Party, and any breaches of these safeguards.

113. The reports submitted may also indicate how much of the information provided by the information provider has been utilised, how it has been used and an assessment of the extent of its usefulness to the information consumer.

Retention of information

114. Information shall be stored in accordance with the information consumer's records retention and disposal schedule.

115. 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; and shall be reviewed annually. The review shall be recorded in writing.

Issues, disputes and resolution

116. Both Parties agree to inform each other immediately, in writing, of any problem arising in respect of this MOU and/or any issues involving the security, legal management, accessibility, storage, processing and/or retention of the information being shared. Likewise both Parties agree to report immediately any instances of breaches to the terms of this MOU and to raise an appropriate security incident.

117. Notification of a breach to this MOU shall be communicated in writing between the relevant individuals at both Parties who are responsible for managing information security incidents, unless it is impractical or inexpedient to do so, in which case, written confirmation should be provided as soon as possible thereafter. Follow up investigation will be the responsibility of the Party where the breach has occurred. Subsequent investigation reports and updates will be communicated to the relevant contact at the other Party.

118. Where a problem arises in respect of this MOU it should be communicated, in writing, between the SPOC at HMRC (listed in **Annex 3**) and the Information Governance Lead at NHS Protect (listed in **Annex 4**). The contacts will endeavour to resolve the problem within 2 working days.

119. Where it is not possible to resolve the issue within 2 working days, or the issue is of such severity that customers may be negatively affected, the issue will be escalated to the Senior Management Team for each Party. They will be notified with an explanation of why the dispute has not been resolved so that they can take appropriate action to resolve the issue or make contingency arrangements.

120. The Senior Management Teams for each Party will attempt to negotiate a settlement in the spirit of joint resolution within 20 working days of a formal notification being received.

121. Any issues regarding ongoing delivery aspects of the information supply, such as data integrity or quality, should be communicated, in writing, between the SPOC at HMRC (listed in **Annex 3**) and the Information Governance Lead at NHS Protect (listed in **Annex 4**).

122. If it is decided that, as a result of frequent problems, amendments to this MOU are required, a formal change notification should be communicated in writing between the Data Exchange Coordinator at HMRC (listed in **Annex 3**) and the Information Governance Lead at NHS Protect (listed in **Annex 4**). External changes affecting the operational delivery responsibilities of the organisations may also necessitate the review and potential amendment of this MOU. Any such amendments will not be made without the written agreement of both Parties.

Costs

123. HMRC will not charge NHS Protect for information requested under the arrangements in this MOU unless the number of requests made per year (ending on 31 March each year) by NHS Protect exceeds 50. Should NHS Protect make more than 50 requests HMRC may decide to charge an administration fee for all requests made in that year, not just those over the 50.

124. NHS Protect will not charge HMRC for information requested under the arrangements in this MOU unless the number of requests made per year (ending on 31 March each year) by HMRC exceeds 50. Should HMRC make more than 50 requests NHS Protect may decide to charge an administration fee for all requests made in that year, not just those over the 50.

125. For these purposes each individual or company named on a request counts as a separate request.

Terms and review arrangements

126. This MOU shall commence on the date of its signature by the Parties and remain in effect for a term of one year.

127. This MOU will be formally reviewed after one year, and thereafter on an annual basis, by both Parties to the MOU.

128. The Parties may agree to review this MOU more frequently to resolve any matters or concerns arising out of the operation of the MOU upon the written request of either Party.

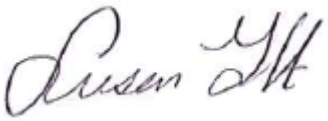
129. Either Party may terminate, re-negotiate or withdraw from this MOU at any time upon giving the other Party at least one month's notice in writing of its intention to do so.

130. The duty of confidentiality relating to any confidential information shared under this MOU may continue after the MOU is terminated. Both Parties agree to continue to apply the principles of this MOU to any information they continue to hold, and which was obtained under this MOU, after the termination of the MOU.

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

Signatories to this MOU

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

Signed for and on behalf of **HM Revenue and Customs**		**Signed for and on behalf of** **NHS Protect** **NHS Counter Fraud Services**	
Signed		Signed	
Name	Euan Stewart	Name	Sue Frith
Title	Deputy Director Risk and Intelligence	Title	Managing Director
Date	07/05/2015	Date	24/03/2015

133. This MOU is made on the 7 of May 2015.

Annex 1

HMRC to NHS Protect sample request form

Restricted

Request for disclosure of personal data by HM Revenue and Customs.

Protective marking	Official – sensitive ☐	Secret ☐	Top secret ☐

Requesting officer	
Address	
Email address	
Telephone number	
Date	

The following request is required to assist in enquiries which are concerned with and/or are for the purposes of (please tick one box only, see note 2):

Data Protection Act 1998 - Section 29(3) crime exemption	
☐	the prevention or detection of crime
☐	the apprehension or prosecution of offenders
☐	the assessment or collection of any tax or duty

Please provide information concerning the following individual (see note 3):

Full name	
Full address	
Date of birth	
Other relevant information as appropriate	

Nature of enquiry

I require the following information (see note 4):

The information is required for the following investigation (see note 5):

HMRC reference (see note 6):

Please give brief details to show that:

- the requested information cannot be obtained by other means or from other sources
- the requested information will be of substantial value to the investigation or proceedings
- lack of access to the requested information will prejudice the investigation or proceedings

I have reasonable grounds for believing that failure to disclose this information will be likely to prejudice those matters and confirm that it will not be used in any way incompatible with the purpose for which it is being disclosed. I understand that if any information on this form is omitted or wrong, I may be committing an offence under Section 55 of the Data Protection Act 1998 (see note 7).

Investigating officer	
Signature	
Date	
Authorising officer	
Signature	
Date	

Notes

Note 1 Please provide the name of the organisation/company from which you are requesting information.

Note 2 Please tick one box under Section 29(3) (crime exemption). This exemption can be used if you are requesting information to support criminal investigations. Exemption 29(3) provides that personal data are exempt in any case, in which the disclosure is for any of the crime (and taxation) purposes and where the application of those provisions in relation to the disclosure would be likely to prejudice any of the matters mentioned.

Note 3 Please supply sufficient information for the Data Protection Controller to identify an individual on their records. You should include the name of the individual in all circumstances and any other relevant information. If possible, in order to assist the Data Controller, you should include a copy of any documentation which supports and confirms the details supplied.

Note 4 Please state what information you require to support your enquiry. You should not ask for "all information known about the individual" or similar. Additionally, you must ask for specific information, if in doubt discuss the matter with the Data Controller.

Note 5 Please give enough information so that the Data Controller can make a decision whether to disclose in accordance with your declaration. This information must relate to the specific enquiry, including a clear explanation as to why the information is being sought and why the enquiry is likely to be prejudiced if it is not provided.

Note 6 Please supply the case number, file number, case name, or any other reference that identifies the investigation.

Note 7 This form should not be used where the only purpose is to confirm known facts, for general intelligence or for administrative functions. The Investigating and Authorising Officers should be aware that they are each making a statement that the two conditions are true and that obtaining personal data under false pretences may be a criminal offence.

Extracts from the Data Protection Act 1998

S. 1 Basic interpretative provisions

(1) In this Act, unless the context otherwise requires—

"data" means information which—

(a) is being processed by means of equipment operating automatically in response to instructions given for that purpose,

(b) is recorded with the intention that it should be processed by means of such equipment,

(c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system, or

(d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record as defined by section 68;

S. 29 Crime and taxation

(1) Personal data processed for any of the following purposes—

(a) the prevention or detection of crime,

(b) the apprehension or prosecution of offenders, or

(c) the assessment or collection of any tax or duty or of any imposition of a similar nature, are exempt from the first data protection principle (except to the extent to which it requires compliance with the conditions in Schedules 2 and 3) and section 7 in any case to the extent to which the application of those provisions to the data would be likely to prejudice any of the matters mentioned in this subsection.

(2) Personal data which—

(a) is processed for the purpose of discharging statutory functions, and

(b) consist of information obtained for such a purpose from a person who had it in his possession for any of the purposes mentioned in subsection (1), are exempt from the subject information provisions to the same extent as personal data processed for any of the purposes mentioned in that subsection.

(3) Personal data are exempt from the non-disclosure provisions in any case in which—

(a) the disclosure is for any of the purposes mentioned in subsection (1), and

(b) the application of those provisions in relation to the disclosure would be likely to prejudice any of the matters mentioned in that subsection.

(4) Personal data in respect of which the data controller is a relevant authority and which—

(a) consist of a classification applied to the data subject as part of a system of risk assessment which is operated by that authority for either of the following purposes—

(i) the assessment or collection of any tax or duty or any imposition of a similar nature, or

(ii) the prevention or detection of crime, or apprehension or prosecution of offenders, where the offence concerned involves any unlawful claim for any payment out of, or any unlawful application of, public funds, and

(b) are processed for either of those purposes, are exempt from section 7 to the extent to which the exemption is required in the interests of the operation of the system.

(5) In subsection (4)—

"public funds" includes funds provided by any Community institution;

"relevant authority" means—

(a) a government department,

(b) a local authority, or

(c) any other authority administering housing benefit or council tax benefit.

Annex 2

Document control

Personnel

Key personnel	Name	Organisation (team)
Authors	Peter McCafferty Paul Wilson	HMRC NHS Protect
Approvers	External Data Exchange Team Information Policy and Disclosure Team RIS Data Guardian Information Governance Team Information and Intelligence Unit National Investigation Service Local Support and Development Service	HMRC HMRC HMRC NHS Protect NHS Protect NHS Protect NHS Protect
Review control	Peter McCafferty Paul Wilson	HMRC NHS Protect

Version history

Version	Date	Summary of changes	Changes marked
0.1	03/06/2014		
0.2	30/01/2015		Yes
0.3	02/03/2015	Version 0.2 changes accepted	No
0.4			
0.5			

Review dates

Version	Publication date	Review date
1.0	06/03/15	06/03/16

Annex 3

HMRC contacts

Gateway Exchange Team (GET)
Single Point of Contact (SPOC)

Judith Hall
HMRC
Room G72
Gateway Exchange Team
CEI Cardiff
Ty-Glas Road
Llanishen
Cardiff
CF14 5TS

T 03000 580 320
E cri.gatewaydisclosure@hmrc.gsi.gov.uk
judith.hall@hmrc.gsi.gov.uk

Escalation within GET
Responsibility: escalation within HMRC

T 03000 586 240
E florence.tennent@hmrc.gsi.gov.uk

Security and Information Team
Responsibility: security incidents

E dan.leonard@hmrc.gsi.gov.uk

Policy and Disclosure Team
Responsibility: legal issues

E ccp.disclosure@hmrc.gsi.gov.uk

External Data Exchange Team
Responsibility: EDE process and MOUs

E john.kershaw@hmrc.gsi.gov.uk

Freedom of Information Team
Responsibility: freedom of information requests

E foi.request@hmrc.gsi.gov.uk

Chief Digital and Information Officer Group
Responsibility: data exchange champion

E peter.carver@hmrc.gsi.gov.uk

Annex 4

NHS Protect contacts

Authorising Officers for Senior Intelligence Officers

Intelligence and Research Development Manager

Chris Cockell
Fourth Floor Skipton House
80 London Road
London
SE1 6LH

M 07715 369 887
E Chris.Cockell@nhsprotect.gsi.gov.uk

Central Intelligence Lead

David Evans
Fourth Floor Skipton House
80 London Road
London
SE1 6LH

M 07768 711 475
E David.Evans@nhsprotect.gsi.gov.uk

Senior Intelligence Officers

Kate Smith
Fourth Floor Skipton House
80 London Road
London
SE1 6LH

T 020 7895 4678
E Kate.Smith@nhsprotect.gsi.gov.uk

Janet Logan
Fourth Floor Skipton House
80 London Road
London
SE1 6LH

T 020 7895 4679
E Janet.Logan@nhsprotect.gsi.gov.uk

Laura Cunningham
Fourth Floor Skipton House
80 London Road
London
SE1 6LH

T 020 7895 4587
E Laura.Cunningham@nhsprotect.gsi.gov.uk

Ji Lamey
Fourth Floor Skipton House
80 London Road
London
SE1 6LH

T 020 7895 4607
E Ji.Lamey@nhsprotect.gsi.gov.uk

John Cunningham
Fourth Floor Skipton House
80 London Road
London
SE1 6LH

T 020 7895 4681
E John.Cunningham@nhsprotect.gsi.gov.uk

Janet Maddison
First Floor Citygate
Gallowgate
Newcastle upon Tyne
Tyne and Wear
NE1 4WH

T 0191 204 6343
E Janet.Maddison@nhsprotect.gsi.gov.uk

Authorising Officers for Area Anti Fraud Specialists

National Investigation Service (NIS) Manager

Derek Johnson
First Floor Citygate
Gallowgate
Newcastle upon Tyne
Tyne and Wear
NE1 4WH

M 07967 273 753
E Derek.Johnson@nhsprotect.gsi.gov.uk

Area Manager Anti Fraud

Kevin Cane
Fourth Floor Skipton House
80 London Road
London
SE1 6LH

M 07833 584 095
E Kevin.Cane@nhsprotect.gsi.gov.uk

Anti Fraud Lead (NIS North)

David Hall
First Floor Citygate
Gallowgate
Newcastle upon Tyne
Tyne and Wear
NE1 4WH

M 07768 647 744
E David.Hall@nhsprotect.gsi.gov.uk

Anti Fraud Lead (NIS South)

Mick Hayes
Fourth Floor Skipton House
80 London Road
London
SE1 6LH

M 07715 369 880
E Mick.Hayes@nhsprotect.gsi.gov.uk

Area Anti Fraud Specialists

1 Northern and Yorkshire

Amanda Hill
First Floor Citygate
Gallowgate
Newcastle upon Tyne
Tyne and Wear
NE1 4WH

M 07710 152 272
E Amanda.Hill@nhsprotect.gsi.gov.uk

2 North West

Pauline Smith
Third Floor Lakeside
Alexandra Park
St Helens
WA10 3TL

M 07715 160 745
E Pauline.Smith@nhsprotect.gsi.gov.uk

3 East Midlands

Jane Stevenson
Fourth Floor Skipton House
80 London Road
London
SE1 6LH

M 07974 653 184
E Jane.Stevenson@nhsprotect.gsi.gov.uk

4 West Midlands

Reg Madden-Waite
Cheylesmore House North
5 Quinton Road
Coventry
West Midlands
CV1 2WT

M 07825 119 251
E Reg.Madden-Waite@nhsprotect.gsi.gov.uk

5 Eastern

Patrick Kelly
Fourth Floor Skipton House
80 London Road
London
SE1 6LH

M 07798 826 512
E Patrick.Kelly@nhsprotect.gsi.gov.uk

6 London

Mark Howard
Fourth Floor Skipton House
80 London Road
London
SE1 6LH

M 07884 314 326
E Mark.Howard@nhsprotect.gsi.gov.uk

7 South East

Nicole McLaughlin
Fourth Floor Skipton House
80 London Road
London
SE1 6LH

M 07715 369 886
E Nicole.McLaughlin@nhsprotect.gsi.gov.uk

8 South West

Debbie Cole
Fourth Floor Skipton House
80 London Road
London
SE1 6LH

M 07967 713 009
E Debbie.Cole@nhsprotect.gsi.gov.uk

9 Wales

Graham Dainty (Operational Fraud Manager)
Mamhilad House
Mamhilad Park Estate
Pontypool
Wales
NP4 0YP

M 07764 354 267
07767 634 016
E Graham.Dainty@nhsprotect.gsi.gov.uk

Information Governance

Information Governance Lead

Ivana Bartoletti
Fourth Floor Skipton House
80 London Road
London
SE1 6LH

M 07931 959 521
E Ivana.Bartoletti@nhsprotect.gsi.gov.uk

Responsibilities:

security incidents
legal issues
EDE process and MOUs
freedom of information requests
subject access requests
access to information complaints
escalation within NHS Protect

Annex 5

Glossary

List of terms and abbreviations used in this document

AAFS	Area Anti Fraud Specialist (NHS Protect)
ACPO	Association of Chief Police Officers
AFL	Anti Fraud Lead (NHS Protect)
AFS	Anti Fraud Specialist (NHS Protect)
ATCSA	Anti Terrorism Crime and Security Act 2001
COP	Anti Terrorism Crime and Security Act 2001: Code of Practice on the Disclosure of Information
CPIA	Criminal Procedures and Investigations Act 1996
CPS	Crown Prosecution Service
CRCA	Commissioners for Revenue and Customs Act 2005
DOF	Director of Finance
DPA	Data Protection Act 1998
ECHR	European Convention on Human Rights
ECU	Economic Crime Unit
FOI	Freedom of Information Act 2000
GET	Gateway Exchange Team (HMRC)
GSC	Government Security Classification System
GSI	Government Secure Intranet
HMRC	Her Majesty's Revenue and Customs
HRA	Human Rights Act 1998
LCFS	Local Counter Fraud Specialist (NHS)
MG	Manual of Guidance (MG forms)
MOU	Memorandum of Understanding
NFS	National File Standards (Crown Prosecution Service)
NIS	National Investigation Service (NHS Protect)
PACE	Police and Criminal Evidence Act 1984
PEACE	Planning and Preparation, Engage and Explain, Account, Closure, Evaluation
PLO	Police Liaison Officer
PNC	Police National Computer
PSB	Public Sector Body
RIPA	Regulation of Investigatory Powers Act 1998
SPF	Security Policy Framework
SPOC	Single Point of Contact

Data controller	has the meaning set out in section 1 of the Data Protection Act 1998, i.e. 'a [natural or legal] person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed'.
Data processor	has the meaning set out in section 1 of the Data Protection Act 1998, i.e. 'in relation to personal data, any [natural or legal] person who processes the data on

behalf of the data controller'.

Data protection legislation	means the Data Protection Act 1998, the EU Data Protection Directive 95/46/EC, the Regulation of Investigatory Powers Act 2000, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (SI 2000/2699), the Electronic Communications Data Protection Directive 2002/58/EC, the Privacy and Electronic Communications (EC Directive) Regulations 2003 and all applicable laws and regulations relating to processing of personal data and privacy, including where applicable the guidance and codes of practice issued by the Information Commissioner.
Freedom of information legislation	means the Freedom of Information Act 2000 and any subordinate legislation made under this Act together with any guidance and/or codes of practice issued by the Information Commissioner or relevant Government Department in relation to such legislation.