INFORMATION SHARING AGREEMENT

between
NHS Shared Business Services
and
NHS Protect

Between

(1) **NHS Shared Business Services**
Phoenix House, Topcliffe Lane, Tingley, Wakefield, WF3 1WE;

acting as data processor for and on behalf of individual health body clients, including but not limited to Department of Health, NHS Trusts, Foundation Trusts, Mental Health Trusts, Clinical Commissioning Groups, NHS England (including Commissioning Support Units, Regional Teams and Local Area Teams) and Arms Length Bodies; and

(2) **NHS Protect**
Fourth Floor, Skipton House, 80 London Road, London, SE1 6LH

being collectively 'the Parties'.

Purpose of agreement

1. 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.

2. 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.

3. The terms 'information' or 'data' is used in this Agreement to refer to any and all information or data used for NHS 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.

NHS Shared Business Services

4. NHS Shared Business Services is a public-private partnership organisation providing services to the NHS which, following the NHS review in April 2013, amounts to the processing of NHS revenue valued at several billion per year. NHS Shared Business Services provides finance and accounting services for NHS England and all the constituent parts of NHS commissioning in England (Regional Teams, Area Teams, Clinical Commissioning Groups and Commissioning Support Units), which means the majority of money spent on NHS commissioning in England will be processed by NHS Shared Business Services. Services include but are not limited to:

   - Finance and accounting
   - Employment (including payroll and pensions)
   - Procurement (including invoice processing)
   - Primary care services (including ophthalmic payments and finance management for GPs)
   - NHS debt recoveries

NHS Protect

5. 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. NHS Protect leads on work to identify and tackle crime across the NHS. Its purpose is to safeguard NHS resources so that the NHS is better equipped to care for the nation's health. NHS Protect leads work to protect NHS staff, patients and resources by providing support, guidance and direction to the NHS. 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.

Working together

6. As NHS Shared Business Services expands its relationship with NHS England, processing invoices, claims and payments for the majority of the NHS including Foundation Trusts, Clinical Commissioning Groups and Arms Length Bodies, then potentially NHS Shared Business Services may feature heavily as a source of intelligence in NHS Protect investigations going forward. As NHS Shared Business Services are currently processing NHS revenues worth several billion per year, then even a small percentage of fraudulent transactions would represent a potentially significant amount of revenue loss to the NHS. Through the development of this Agreement, NHS Shared Business Services can greatly assist NHS Protect in the prevention and detection of fraud.

Types of information

7. 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.

8. 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 data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.' 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. 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 Agreement, 'personal' includes the Data Protection Act 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.

Data control

9. 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.

10. For the purpose of this Agreement, NHS Shared Business Services is a 'data processor' engaged in processing NHS information for and on behalf of individual health body clients, including but not limited to Department of Health, NHS Trusts, Foundation Trusts, Mental Health Trusts, Clinical Commissioning Groups, NHS England (including Commissioning Support Units, Regional Teams and Local Area Teams) and Arms Length Bodies.

Sharing framework

11. The Parties agree and acknowledge that they each receive, gather and store information. Where the Parties decide to share information with each other, it will share that information according to the Information Sharing Agreement described below 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/2013/12/sec-b-cond-1415.pdf

12. The Parties agree to share information with each other in order to assist with anti-fraud work (for example to identify fraudulent or suspicious invoices for NHS payment, to establish fraud trends in the procurement process based on specific projects or targeted areas, to identify individuals or companies suspected of fraud and to prevent fraudulent or similarly inappropriate payments from being made).

13. When the giving Party discloses information to the receiving Party, that information shall be disclosed for the purposes of the prevention, detection, investigation and prosecution of fraud or any other unlawful activity affecting the NHS, as set out in the NHS Business Services Authority Directions 2006, which can be found at:

    http://www.nhsbsa.nhs.uk/Documents/Sect_1_-_B1_-_Eng_Directions.pdf

14. Where the giving Party shares information with the receiving Party, it may share the information in any 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.

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

16. 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.

17. 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 paragraphs 18-20), whether in hard-copy or electronic format, held by either Party, will be stored securely.

Information sharing agreement

18. Information disclosed by either Party will comply with the Government Security Classification System (GSC)[1], 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, 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

19. 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.

20. 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 giving Party, except in the form of non-disclosive statistical data, anonymised data or conclusions;
    b. use the information for any commercial, industrial or other purpose; or
    c. copy, adapt, duplicate or otherwise reproduce the information save as provided in this Agreement.

21. If there is a need for either Party to disclose or supply information to other 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

22. 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

[1] This supersedes the Government Protective Marking Scheme (GPMS), which has six levels of marking: "Top Secret", "Secret", "Confidential", "Restricted", "Protect" and "Not Protectively Marked" (or "Unclassified").

shared information is accurate, necessary, secure, legal and ethical, taking into account relevant legislation where applicable, including:

- Health and Social Care Act 2012;
- NHS Act 2006;
- Freedom of Information Act 2000;
- Data Protection Act 1998;
- Human Rights Act 1998;
- Disability Discrimination Act 1995;
- Access to Health Records Act 1990.

23. 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 fraud and other unlawful activities. It is therefore appropriate that information relating to the administration of NHS business may be used for these purposes provided that the requirements of law and policy are satisfied.

24. Information shared between the Parties will only be used for the purpose(s) specified in this Agreement and its use 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

25. 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 or data from an NHS contractor (defined as any person or organisation providing services of any description under arrangements made with an NHS body) in connection with the exercise of the Secretary of State for Health's counter fraud functions.

26. 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.

27. The disclosure of information or data by NHS Shared Business Services 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 with regard to the anti-fraud requirements in the NHS Standard Contract. 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

    - NHS Standard Contract:
      http://www.england.nhs.uk/wp-content/uploads/2013/12/sec-b-cond-1415.pdf

28. Information or data supplied by NHS Shared Business Services to NHS Protect may be used by NHS Protect 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.

29. NHS Protect, as a public sector health body, is subject to the Freedom of Information Act 2000. Therefore the disclosure of information by NHS Protect is subject to Freedom of Information provisions. The principles of the Freedom of Information Act 2000 apply and nothing provided in this Agreement is confidential to either Party to this Agreement.

30. Under the Freedom of Information Act 2000, individuals can make a request to NHS Protect for information to be disclosed. This is called a Freedom of Information Request. Requests must be put in writing to NHS Protect following the official Freedom of Information Request process. Requests will be considered by the Information Governance Lead at NHS Protect and a decision will be made as to the legality and appropriateness of information disclosure. For requests concerning other parties, including but not limited to NHS Shared Business Services, NHS Protect will ensure consultation is made where information relates to the operations of NHS Shared Business Services.

31. NHS Protect is also 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. Requests must be put in writing to NHS Protect following the official Subject Access Request process. Requests will be considered by the Information Governance Lead at NHS Protect and a decision will be made as to the legality and appropriateness of information disclosure.

32. 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.

33. NHS Shared Business Services is a private limited company and so is not subject to the Freedom of Information Act 2000. Additionally NHS Shared Business Services, as the data processor working for and on behalf of NHS clients (data controllers), does not have the same ownership responsibilities as data controllers.

34. Information relating to NHS business processed by NHS Shared Business Services is essentially public sector information; therefore this information may be subject to Freedom of Information and Subject Access enquiries but only by going through the health body client's own Freedom of Information Request or Subject Access Request processes. It is up to the health body client to disclose information, or to authorise the disclosure of information, under the terms of the Freedom of Information Act 2000 or the Data Protection Act 1998.

35. Public sector information, which is subject to the provisions of the Freedom of Information Act 2000 and the Data Protection Act 1998, should not be accessed under Freedom of Information or Subject Access processes by going directly to a third party data processor, such as NHS Shared Business Services.

36. 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

37. NHS Shared Business Services and NHS Protect, as functional administrators of NHS business, 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

NHS Shared Business Services	Registration number: **Z8954005**
NHS Protect	Registration number: **Z9395747**

38. 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 processors 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.

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

    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

40. Each Party's responsible officer for information governance 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.

41. 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 central government as 'Restricted' (see paragraphs 17-19). 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.

42. 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;
- Appropriate security on external routes into the organisation, for example internet firewalls and secure dial-in facilities.

43. 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.

44. 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 via GSI or NHS.net networks) and, if posted, will be encrypted to approved standards to protect the information and dispatched by Royal Mail Special Delivery service or by courier.

45. 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.

46. 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.

47. Both Parties reserve the right to conduct an on-site audit of confidentiality and security procedures and practices for guaranteeing the security and confidentiality of the information covered by this Agreement.

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

Breach and dispute procedures

49. Both Parties agree to report immediately instances of breaches between the giving and receiving Parties to any of the terms of this Agreement and to raise an appropriate security incident.

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

Point of contact

51. The Parties agree to, when 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).

52. 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 an NHS Protect 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 fraud investigations 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.

53. NHS Shared Business Services will appoint an accredited Counter Fraud Specialist (or ensure an existing member of staff undergoes counter fraud training and accreditation); this person will be NHS Shared Business Services' nominated single point of contact for investigation purposes.

54. 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 (via GSI or NHS.net networks). 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.

55. 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 via NHS.net systems, 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.

56. The single point of contact for NHS Shared Business Services (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 NHS Protect investigation) will be:

Name	Evelyn Thomas
Title	Head of Audit
Address	NHS Shared Business Services, Phoenix House, Topcliffe Lane, Tingley, Wakefield, WF3 1WE
Phone	01179 338 732
Email	Evelyn.Thomas2@nhs.net

57. The single point of contact at Shared Business Services for day-to-day communication and/or joint-working in the event of an NHS Protect investigation will be:

Name	Dharika Ruparel
Title	Senior Audit Coordinator and Local Counter Fraud Specialist
Address	NHS Shared Business Services, Phoenix House, Topcliffe Lane, Tingley, Wakefield, WF3 1WE
Phone	07834 420 784
Email	Dharika.Ruparel@nhs.net

58. The single point of contact for NHS Protect (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 NHS Protect investigation) will be:

Name	Amanda Hill
Title	Area Anti Fraud Specialist
Address	NHS Protect, 1st Floor Citygate, Gallowgate, Newcastle upon Tyne, Tyne and Wear, NE1 4WH
Phone	0191 204 6336
Email	Amanda.Hill@nhsprotect.gsi.gov.uk

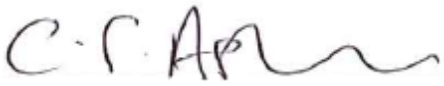
Term of agreement

59. This Agreement shall commence on the date of its signature by the Parties and remain in effect for a term of one year. Upon expiry, the Agreement shall automatically renew for a further period of one year, and thereafter on each anniversary of the Agreement commencing, unless terminated or re-negotiated by either Party.

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

61. This Agreement is not legally binding and is not intended to create legal relationships between the Parties.

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

Signed for and on behalf of	
NHS Shared Business Services	
Signed	
Name	Christopher Ashburn
Title	Chief Financial Officer
Date	14/07/2014

Signed for and on behalf of	
NHS Protect	
Signed	
Name	Dermid McCausland
Title	Managing Director
Date	02/07/2014

63. This Agreement is made on the 14 of July 2014.