Information Sharing Agreement

INTERPRETATION

The words below shall have the following meaning within this agreement:

Agreement, means this Information Sharing Agreement and its accompanying Schedule(s) and Annexes.

Commission, means the Care Quality Commission established under section 1(1) of the Health and Social Care Act 2008.

GDPR, means the General Data Protection Regulation, Regulation (EU) 2016/679

Data subject, means an identified or identifiable natural person as per article 4(1) of GDPR

Partner organisations or **parties,** means the Care Quality Commission, and the Independent Sector Complaints Adjudication Service.

Information Consumer, means the party or parties who receive the information.

Information Provider, means the party or parties who provide the information.

Personal data, means any information relating to an identified or identifiable living person ('data subject'); an identifiable living person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that living person. The obtaining, handling, use and disclosure of such information is principally governed by the General Data Protection Regulation 2016/679 and the Data Protection Act 2018, Article 8 of the Human Rights Act 1998, and the common law duty of confidentiality.

Special category personal data, **Special category personal data**, means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. Special category personal data can only be processed when a condition at article 9(2) applies.

Consent, means a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement (see recital 32 of GDPR).

Confidential Personal Information (CPI), means information that relates to an individual who can be identified from that information or that information and other information which is in the possession of the Commission, and which was obtained by the Commission on terms

or in circumstances requiring it to be held in confidence. Other than for a set of defined purposes, it is a criminal offence under the Health and Social Care Act 2008 for the Commission (or a person authorised by the Commission) to deliberately or recklessly disclose CPI.

Identifiable information, means information that relates to a living or deceased individual who can be identified from that information or that information and other information which is in the possession of, or likely to come into the possession of the Information Provider or Information Consumer.

INTRODUCTION

1. The purpose of this document is to facilitate the lawful, appropriate and effective sharing of information between the partner organisations.

2. The Schedule(s) set out the nature and extent of the information to be shared; the purpose and the identity of the Information Consumer and Information Provider. A party may be an Information Consumer and Information Provider in relation to this Agreement.

3. This Agreement defines the principles and procedures that the Parties shall adhere to whenever they need to share information and the responsibilities each party owes in respect of the other.

4. This Agreement is not enforceable in law and does not override or amend the existing statutory or common law responsibilities and functions of CQC and the Independent Sector Complaints Adjudication Service.

THE PARTNER ORGANISATIONS

Independent Sector Complaints Adjudication Service

5. ISCAS is the recognised complaints management framework in the independent healthcare sector. ISCAS is a voluntary subscription scheme that includes the vast majority of all independent healthcare providers across the UK. The remit has recently been extended to include Private Patient Units (PPUs) and providers of Independent Ambulance Services. Since 2016 ISCAS has operated independently of any trade association and is currently hosted by the Centre for Effective Dispute Resolution (CEDR).

The Care Quality Commission

6. The Commission is the independent regulator of health and social care services in England. It also monitors the use of the Mental Health Act 1983 and protects the interests of people whose rights are restricted under that Act.

7. The Commission was established by the Health and Social Care Act 2008. Its main powers and responsibilities are provided under that Act, the Health and Social Care Act 2012, the Mental Health Act 1983, the Health and Safety at Work Act 1974, and regulations under those Acts.

8. The purpose of the Commission is to make sure health and social care services provide people with the safe, high quality care that they have a right to expect. The Commission expects those services to continuously improve. The Commission's role in this is to ensure providers are meeting fundamental standards. It is the primary duty of hospitals, care homes and other providers of health and social care services to ensure their services improve.

THE PURPOSE(S) FOR THE SHARING OF INFORMATION BETWEEN THE PARTIES

9. The parties to this agreement agree to lawfully and appropriately share information for reasons of public interest in order to ensure high standards of quality and safety of health care.

10. 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 as Schedules of this agreement.

11. A list of these Schedules can be found at Annex 3 of this agreement.

LEGAL REQUIREMENTS

12. Partner organisations must comply with all relevant legal requirements relating to the processing of information (particularly personal data and Indentifiable Information).

13. The principal legislation is listed below and further explained in:

- Data Protection Act 2018
- The General Data Protection Regulation (2016/679)
- Human Rights Act 1998 (Article 8)
- Freedom of Information Act 2000
- Computer Misuse Act 1990
- Health and Social Care Act 2008
- Health and Social Care Act 2012

14. Other legislation may be relevant when sharing specific information.

15. Partner organisations must also comply with the common law duty of confidentiality.

16. The Commission publishes a Code of Practice on Confidential Personal Information, which sets out the practice that the Commission will follow in order to ensure compliance with these legal responsibilities in relation to CPI.

RESPONSIBILITIES

General responsibilities

17. Each Partner Organisation is responsible for ensuring that their organisational, technological and security measures meet the requirements of this agreement.

18. Each Partner Organisation is responsible for ensuring that the requirements of this agreement are appropriately and adequately communicated to their staff, and to other agents acting on their behalf, and for ensuring compliance with this agreement.

19. Each Partner Organisation remains responsible for ensuring their own compliance with applicable legislation and common law. If they consider that any part of this agreement is incompatible with that requirement, then compliance with the law takes precedence. In such circumstances, they must notify all parties as soon as possible.

Personal data (including special category personal data), CPI and Identifiable information

20. Staff must only be given access to personal data, CPI and Identifying data where that access is necessary in order for them to perform their duties.

21. Personal data, CPI and Identifiable information must only be shared between partner organisations where:

    a) There is a lawful basis to do so,

    b) The organisation receiving the personal data, CPI and Identifiable information has a genuine and legitimate 'need to know', and

    c) The disclosure is considered proportionate, with consideration of the potential impact upon the privacy of individuals.

22. Where ever possible, consideration should be given as to whether it is necessary to share or use personal data, CPI and identifiable information. Where non-personal, anonymised or pseudonymised data can be practicably be used instead, then personal data, CPI and identifiable information must not be shared or used.

23. Each partner organisation must ensure that any of its employees or agents accessing personal data and CPI is fully aware of their responsibilities to maintain the security and confidentiality of personal data.

24. Each partner organisation must take reasonable steps to ensure that any of its staff accessing personal data, CPI and identifiable information (that has been shared under this Information Sharing Protocol) follow the procedures and standards that have been agreed and incorporated within it.

25. Personal data must not be transferred to a third country or international organisation unless the conditions laid down in Chapter 5 of GDPR are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. Information obtained under this protocol must not be transferred to third country or international organisation without the explicit consent of the data subject (the person to whom the information relates) and/or the permission of the Information Provider.

Consent (in relation to personal data, CPI and Identifying data)

26. Consent is one condition that will permit the disclosure of personal data under Article 6 of GDPR, or CPI under section 77 or 79 of the Health and Social Care Act 2008. When disclosing special category personal data using the consent condition the consent must be 'explicit' as per Article 9(2)(a). Therefore, when using consent as the basis for disclosure of special category personal data, particular care should be taken to ensure that the data

subject is fully informed as to what data it is proposed to disclose, with whom, for what purpose, and how that data will be handled and used.

27. Consent is not the only condition for disclosure. Consideration should be given as to whether or not to seek consent if other conditions for disclosure (see below) apply. If consent is sought and refused, it is unlikely to be lawful to subsequently disclose that personal data.

28. The data subject (the person to whom the information relates) has the right to withdraw consent at any time. Sharing or disclosure of personal data must cease if consent, upon which that sharing relied, is withdrawn. Withdrawal of consent must be communicated to the other parties as soon as possible. Following the withdrawal of consent, all parties must assess whether another condition under article 6 of GDPR (and article 9 for special personal data) will lawfully apply to allow them to continue processing that personal data (see below).

29. Where the data subject is an aged over 13 years old, and does not have the capacity to give informed consent, no other person may give consent on their behalf unless specifically empowered to do so by power of attorney or order of a court. In such circumstances, personal data may only be shared where another condition under article 6 of GDPR (and article 9 for special personal data) will lawfully apply to permit this.

30. Consideration should also be given as to whether it is possible and appropriate to seek the consent to disclose from each person whose personal data is being disclosed. Where it is not possible or appropriate to do so, then it is the responsibility of the Information Provider to satisfy themselves that another condition (or conditions) under article 6 of GDPR (and article 9 for special personal data) applies and makes the disclosure lawful.

Disclosure of personal data (including sensitive personal data) without consent.

Personal data may only be disclosed (or otherwise processed) without consent where processing is lawful and a condition under article 6(1) of GDPR applies.

Special category personal data must not be processed. The only exception to this is where a condition at article 9(2) applies to the processing having regard to Schedule 1 of the Data Protection Act 2018 where appropriate.

31. **Identifiable Information** will be processed in line with the Commissions policy on Confidential Personal Information. Where identifiable information is not directly identifiable, the data consumer will not attempt to further identify individuals using any other data sources including information in the public domain.

32. **Confidential Personal Information** can only be disclosed by the Commission without consent where the person making the disclosure can *prove that they reasonably believed*:
    - That the information had previously been lawfully disclosed to the public;
    - That the disclosure was made under or pursuant to regulations under section 113 or 114 of the Health and Social Care (Community Health and Standards) Act 2003 (c.43) (complaints about health care or social services)
    - That the disclosure was made in accordance with any enactment or court order;
    - That the disclosure was necessary or expedient for the purposes of protecting the welfare of any individual; or

- That the disclosure was made to any person or body in circumstances where it was necessary or expedient to do so for the purpose of exercising statutory functions of that person or body.

Or where the person making the disclosure can *prove that* it was made:

- for the purpose of facilitating the exercise of any of the Commission's functions;
- in connection with the investigation of a criminal offence; or
- For the purpose of criminal proceedings.

33. Personal data, sensitive personal data, identifiable information and confidential personal information can be shared between the parties where that data has been adequately anonymised or pseudonymised.

Anonymised and pseudonymised data

34. For the purposes of this section, pseudonymised data that could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person and would be subject to the principles of data protection (see recital 26 of GDPR).

35. For the purposes of this section, anonymised data which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable is not subject the principles of data protection (see recital 26 of GDPR).

36. In order to protect privacy, reduce the risks relating to GDPR compliance and to minimise the risk of security breaches, data being used by and shared between the partner organisations should be anonymised wherever possible.

37. Anonymised data about an individual can be shared without consent in a form where the identity of the individual cannot be recognised i.e. when:

- Reference to any data item that could lead to an individual being identified has been removed;
- The data cannot be combined with any data sources held by any likely recipient in order to produce personal identifiable data (i.e. where nobody who is likely to receive the data could reasonably be able to identify individuals from that data, on its own or when combined with other information available to them, or likely to become available to them).

38. The anonymisation of personal data for sharing should be carried out with regard to the Information Commissioner's Anonymisation Code of Practice.

39. It is the responsibility of the provider organisation to ensure that any anonymisation of personal data is adequate in accordance with this Code.

40. Where the Information Consumer intends to publish or further disclose anonymised health or social care information, it is their responsibility to ensure that it is anonymised in accordance with Information Standard ISB 1523 – Anonymisation Standard for Publishing Health and Social Care Data

41. The Information Consumer must not attempt to identify individuals from anonymised information, or to combine or link anonymised information with any other information in

such a way as to make it reasonably possible to identify individuals, without the written consent of the Information Provider.

Non-personal data

42. Partner organisations should not assume that non-personal information is not sensitive or confidential and can be freely shared. This may not be the case and, where there is any doubt as to whether such information is sensitive or confidential, the Information Provider should be contacted before any further sharing takes place.

Data Quality

43. The Information Provider shall ensure the information it provides is of sufficient quality, namely:

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

Prohibition on Further Use

44. The Information Consumer shall ensure the information provided by the Information Provider is used exclusively for the specified purposes set out in this agreement and shall not further use the information in any manner incompatible with that purpose or purposes without the prior written consent of the Information Provider or as provided by law.

Security Arrangements

45. Partner Organisations will ensure the security of supplied information, personal or non-personal, and process the information accordingly. This will be to article 32 of GDPR and the applicable baseline security standards as detailed in ISO27001.

46. Partner organisations must make it a condition of employment that employees will abide by their rules and policies in relation to the protection and use of personal data and other confidential information. This condition should be written into employment contracts and any failure by an individual to follow the policy should be dealt with in accordance with that organisation's disciplinary procedures.

47. Partner organisations must ensure that their contracts with external service providers comply with article 28 of GDPR in relation to the protection and use of confidential information. Assurances should be obtained that service providers comply with the requirements of ISO27001 or equivalent standards.

48. The Information Provider shall exercise reasonable judgement and apply the appropriate security classification (set out in Annex 2) to any confidential information (including personal data) prior to its onward transmission to the Information Consumer.

49. Information must then be transmitted in accordance with the appropriate level of security marking applied.

50. The security classification shall determine the MINIMUM security measures to be employed to protect the information against unauthorised or unlawful access, accidental

loss or destruction and damage. Parties may choose to apply further measures above and beyond these minimums.

51. The Information Consumer may increase the level of protection afforded to the information but may not decrease it without the express written consent of the Information Provider.

52. The Parties agree to maintain the appropriate security measures throughout the lifecycle of the information, in particular, during storage, use, transmission and destruction.

53. The Parties agree to inform each other immediately and report to the Information Commissioners Officer in line with article 33 of GDPR any personal data breach involving the information that is the subject of this agreement.

54. Notification of the breach shall be communicated in writing unless it is impractical or inexpedient, 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. Investigation reports will be copied to the relevant contact(s) at the other parties to this agreement.

55. The Parties shall maintain, and keep up-to-date, a list of individual(s) responsible for managing information security incidents for their organisation in Annex 1 to this Agreement.

Access to Information Requests

56. The Commission is a public authority for the purposes of access to information legislation such as, but not limited, to the Freedom of Information Act 2000, which confers a general right of access to copies of recorded information held by a public authority.

57. The Parties acknowledge that the information that is the subject of this Agreement, and the Agreement itself, may therefore be subject to disclosure.

58. On receipt of a fully compliant request for information provided by the Information Provider, the Commission, as the Information Consumer, shall:

- in writing, inform the Information Provider of the nature and extent of the request as soon as reasonably practicable,

- afford the Information Provider a reasonable opportunity to comment on the request, and should the Information Provider object to disclosure, consider those objections carefully in light of current guidance and case law,

- in writing, notify the Information Provider of its decision as soon as reasonably practicable, but in any event, before the expiry of the statutory deadline, and

- keep the Information Provider informed of any subsequent developments relating to the request

59. The Information Provider shall:

- respond to the Information Consumer's written notification as soon as reasonably practicable setting out its view on disclosure;

- should it object to disclosure, set out its detailed reasons in writing (including, where relevant, the competing public interest arguments) and communicate it to the Information Consumer as soon as reasonably practicable but in sufficient time to enable the Information Consumer to consider its response and prepare a decision letter,

- afford reasonable advice and assistance to the Information Consumer, as required, to ensure the request is handled in accordance with the governing legislation and within the statutory deadlines.

60. In all instances, the decision as to whether the information should or should not be disclosed rests solely with the Information Consumer as the holder of the information and the recipient of the request.

61. The Information Consumer shall not disclose the identity of the individual making the request to the Information Provider unless it is necessary to discharge its responsibilities under this part of the Agreement and/or lawful under the Data Protection Act 2018 and GDPR.

62. The Parties shall maintain, and keep up-to-date, a list of individual(s) responsible for handling access to information requests, (or qualified to take decisions in respect of these requests) for their organisation in Annex 1 to this Agreement.

Retention Periods

63. The information shall be stored in accordance with the Information Consumer's records retention and disposal schedule.

64. 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.

65. The review shall be recorded in writing.

ADMINISTRATION

66. The Parties shall review this Agreement annually or more frequently where necessary by prior agreement of both Parties.

67. Any partner organisation may withdraw from this agreement at any time, however the duty of confidentiality relating to any confidential information shared under this agreement may continue after the agreement is terminated. Partner organisations agree to continue to apply the principles of this agreement to any information that they hold, and which was obtained under this agreement, after the termination of the agreement.

RESOLUTION OF DISAGREEMENTS

68. The Parties agree to resolve any disagreement arising from this Agreement informally and promptly. in the first instance, by the officers who have day-to-day responsibility for the operation of this Agreement.

69. The disagreement shall be escalated to senior officers, up to, and including the Chief Executive Officers, if it cannot be resolved informally. The Chief Executive Officers shall be jointly responsible for ensuring a mutually satisfactory resolution.

70. Complaints arising from access to information requests shall be dealt with under the Information Consumer's policy of the same.

Signed: 

Tom Ward

Care Quality Commission

Date: 19 November 2018

Signed: 

Sally Taber

Independent Sector Complaints Adjudication Service

Date: 20 November 2018

ANNEX 1

KEY CONTACTS

The Commission

Name	Job Title	Contact Details	Area of Responsibility
Paul Durham	Strategy Manager	paul.durham@cqc.org.uk	• Operational Contact • Lead officer for this Agreement
Simon Richardson	Information Rights Manager	simon.richardson@cqc.org.uk	• Requests for Personal Data. • Access to information requests.
Derek Wilkinson	Information Security Manager	derek.wilkinson@cqc.org.uk	• Information security incidents • Information security standards

Independent Sector Complaints Adjudication Service

Name	Job Title	Contact Details	Area of Responsibility
John-Paul Azzi	Head of Consumer Services (CEDR)	jazzi@cedr.com	• Operational Contact • Lead officer for this Agreement
Graham Massie	Chief Operating Officer (CEDR)	gmassie@cedr.com	• Requests for Personal Data. • Access to information requests.
Graham Massie	Chief Operating Officer (CEDR)	gmassie@cedr.com	• Information security incidents

ANNEX 2

Government Security Classifications

ONE of the following security classifications must be applied to a prominent part of the information; in descending order of significance:

- OFFICIAL - SENSITIVE
- OFFICIAL

All information processed within CQC is deemed to be classified as 'Official' regardless of the associated sensitivity.

There is no requirement to mark ROUTINE documents or emails which contain Official information; however when information is shared subject to an Information Sharing Agreement the appropriate marking should be used.

Any document which contains more sensitive information should be marked as 'Official Sensitive'. If there is any doubt whether information should be protectively marked then the question should be escalated, via line management, to the records and document management or information security teams.

The appropriate security classification is the one that best describes the level of harm that may arise in the event the information is unlawfully or accidentally accessed, disclosed, lost destroyed or damaged.

Security classifications will be used in line with the most recent guidance from the Cabinet Office. Descriptors must not be applied to information that is sent to overseas partners (unless formally agreed in advance) as they are not recognised under any international agreements and are likely to cause confusion.

Reasonable care and judgement must be exercised when choosing the relevant security classification because the security classification determines the security measures to be employed.

Security Classification	Description
OFFICIAL	All information processed within CQC is deemed to be classified as 'Official' regardless of the associated sensitivity. Including - Personal information that is required to be protected under the Data Protection Act (1998) or other legislation (e.g. health records).
OFFICIAL - SENSITIVE	Information which is deemed to be sensitive and is not intended to be released outside of the organisation. This may be sensitive personal information relating to individuals, or commercially sensitive information.

Organisations may apply a DESCRIPTOR to identify certain categories of SENSITIVE information and indicate the need for common sense precautions to limit access.

For example;

- OFFICIAL – SENSITIVE - PERSONAL

  When sharing data of a personal nature the disclosure of which could cause damage to an individual, such as medical records.

- OFFICIAL – SENSITIVE – LEGAL

  Information in connection with any legal proceedings (including prospective legal proceedings), for obtaining legal advice or for establishing, exercising or defending legal rights, such as instructions to counsel.

- OFFICIAL – SENSITIVE – COMMERCIAL
  Commercially or market-sensitive information, including that subject to statutory or regulatory obligations, that may be damaging to if improperly accessed. For example statistics relating to the CQC market oversight function.

ANNEX 3

LIST OF SCHEDULES TO THIS AGREEMENT

Details of agreed transfers of information are attached as schedules to this agreement. Further schedules may be added after the signing of this agreement, but must be signed by a person authorised to do so on behalf of their organisation, and those schedules must be recorded below and attached to the full agreement:

SCHEDULE	REF	DATA TOPIC	SIGNED BY	DATE
SCHEDULE A	CQC/ISCAS:2018-01	**Detailed ISCAS adjudication decisions/ broader information updates**	Tom Ward	19 November 2018
			Sally Taber	20 November 2018
SCHEDULE B				
SCHEDULE C				

SCHEDULE A

Schedule of Information Sharing Agreement
(for information sharing that may include personal data, CPI and Identifying data)

Between: Care Quality Commission (CQC) and Independent Sector Complaints Adjudication Service (ISCAS)

Ref: CQC/ISCAS:2018-01

Data provider: ISCAS	Data consumer: CQC
Contact details: Sally Taber sally.taber@iscas.org.uk	Contact details: Darren Smith darren.smith@cqc.org.uk

Data topic: **Detailed ISCAS adjudication decisions/ broader information updates**

Item	Data period	Data sub-topic/ element
1	Ongoing: as and when produced following adjudication decisions	a) All upheld or partially upheld stage 3 adjudication decisions regarding ISCAS subscribing organisations (with the complainant's details anonymised); and b) For above, accompanying written communication to the provider organisation (with complainant's details anonymised). This will be sent initially as part of a 3-month trial to understand its usefulness as well as to consider its replacing (a) above.
2	Ongoing	c) The names of any provider without an independent adjudication process in place and where ISCAS has advised complainants to contact CQC directly.
3	Monthly/ quarterly updates as stipulated	d) A report in an agreed format that summarises the adjudication decisions (three to four times per year, following each ISCAS Advisory Board meeting); e) An up-to-date report listing the names of all ISCAS subscribing organisations, three to four times per year, following each ISCAS Advisory Board meeting.

Item	Background information (if required)
1	Following completion of this agreement, a 3-month pilot will be conducted where (b) will be offered in addition to (a) followed by a review/ consideration of possibly moving exclusively to (b) unless a request is made for a specific report of (a). **The following text is sent to all ISCAS complainants in England:**

	"ISCAS shares adjudication decisions with the Care Quality Commission (CQC), the regulator of hospitals in England. Your details will be anonymised, but the hospital/organisation will be identified. The CQC considers issues arising from complaints as part of the repository of information it holds on each hospital/organisation and may use this to recommend improvements."
2	Recognition that the highlighted provider appears to have no mechanism to offer an independent review of complaints against its quality of care.
3	

Item	For the following purpose:
1	Each report is made available to: ▪ the CQC inspector responsible for the given provider; and ▪ the CQC qualitative team within Intelligence, as part of the programme of ongoing monitoring of the quality of care provision. More specifically, it offers the inspector an opportunity to understand both the organisation's process for handling complaints as well as reviewing the content for any ongoing themes.
2	Consideration of a provider's registration requirements with regard to acting on complaints (Regulation 16: Receiving and acting on complaints) as well as any wider questions this may pose on the provider's well-led domain.
3	Review of high-level themes for wider complaint handling across all sectors of care

Item	Limitations on use, storage and sharing of the data:
1	ISCAS remove the individual's details before sharing the report. The pilot (discussed above) will review the potential of replacing these reports with the accompanying letter sent to the provider regarding the case. The individual's details will be redacted from each letter. The report/ letter will be sent through the CQC's sftp system and stored on a restricted area of CQC's Y/drive network. CRM enquiries are raised for inspectors with the report featuring as a password-protected attachment. Reports/ letters will be made available to the Intelligence qualitative team for review.
2	No limitation
3	No limitation

Item	Transmission of data – Format/ medium	Proposed date for transfer
1	Secure File Transfer Protocol	Frequency discussed above.
2	Email	Frequency discussed above.
3	Email	Frequency discussed above.

Item	Security Classification (Official / Official – Sensitive / Official – Sensitive – Descriptor)
1	Official – Sensitive – Personal
2	Official
3	Official

Item	Trigger(s) for sharing
1	Production of anonymised reports

2	Determined by frequency (monthly/ quarterly) and in agreement/ correspondence between parties.
3	ISCAS Advisory Board meeting.

Processing of personal data – legal basis:		
Conditions for processing personal data (tick all that apply) – *personal data should only be shared to the extent necessary to achieve the purpose(s)*	N/A (no personal data will be shared other than in anonymised form)	☐
	the data subject has given consent to the processing of his or her personal data for one or more specific purposes;	☐
	processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;	☐
	processing is necessary for compliance with a legal obligation to which the controller is subject;	☐
	processing is necessary in order to protect the vital interests of the data subject or of another natural person;	☐
	processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; (select a sub option below)	
	the administration of justice,	☐
	the exercise of a function of either House of Parliament,	☐
	the exercise of a function conferred on a person by an enactment or rule of law,	☐
	the exercise of a function of the Crown, a Minister of the Crown or a government department, or	☐
	an activity that supports or promotes democratic engagement.	☐
	Legitimate interests of parties to this agreement (explain which legitimate interest(s) and why the processing is justified below. This can only be used in very limited circumstances).	☒
Conditions for processing special category personal data (tick all that apply) – *sensitive*	the data subject has given explicit consent to the processing of those personal data for one or more specified purposes,	☐
	processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of	☐

personal data should only be shared to the extent necessary to achieve the purpose(s)	the data subject in the field of employment and social security and social protection law	
	processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent	☐
	processing relates to personal data which are manifestly made public by the data subject;	☐
	processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;	☐
	processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued	
	Statutory etc and government purposes	☐
	Administration of justice and parliamentary process	☐
	Equality of opportunity or treatment	☐
	Racial and ethnic diversity at senior levels of organisations	☐
	Preventing or detecting unlawful acts	☐
	Protecting the public against dishonesty	☐
	Regulatory requirements relating to unlawful acts and dishonesty	☐
	Preventing fraud	☐
	Support for individuals with a particular disability or medical condition	☐
	Safeguarding of children and of individuals at risk	☐
	Disclosure to elected representatives	☐
	Publication of legal judgements	☐
	processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of	☐

	health or social care systems and services on the basis of Union or Member State law	☒
	processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law	☐
	processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued	
'Defences' for CQC disclosure of Confidential Personal (tick all that apply)	N/A (CQC will not disclose confidential personal information other than in anonymised form)	☒
	Previous lawful disclosure *to the public*	☐
	Disclosure under regulations regarding complaints about health care or social services	☐
	Disclosure required by law (legislation or court order)	☐
	Protecting the welfare of any person	☐
	Exercise of statutory functions (explain which statutory function(s) below)	☐
	Investigation of criminal offences or for purpose of criminal proceedings	☐

Statutory and/or public function(s) being exercised:
The responsibilities of CQC are set out primarily in the Health and Social Care Act 2008 as amended (the 2008 Act) and the accompanying Regulations (as amended). Specific sections of the Act or accompanying regulations will apply, depending on the type of concern. ISCAS provides a formal complaints adjudication process for independently-funded care provision (where the provider is an ISCAS provider). Although not identical, it provides a similar function to that of the NHS Ombudsman for NHS-commissioned care. ISCAS complaints therefore provide CQC with valuable information about the provider's quality of care and internal process for complaint resolution that could not be obtained elsewhere. CQC uses this information to meet its regulatory functions.

Other legitimate interest(s) being served by the sharing of information:
CQC has no alternative method of understanding the type of complaint or underlying details covering the quality of care provision within this part of the independent healthcare sector. This exchange of information allows both the relevant CQC inspectors and Intelligence staff to review the report/ covering letter for possible follow-up action/ use as supplementary information. The sharing of ISCAS complaints information is therefore necessary for CQC to develop this process of review for providers of privately-funded care. Following each stage 2 ISCAS investigation, the finalised report is sent to the complainant. A copy is also sent to the provider organisation along with a covering letter setting out any broad findings. As it is not necessary for CQC to know the complainant's name, ISCAS redact these details from the report and covering letter before sending both to CQC via sftp.

How will individuals be notified of the sharing of personal data:
The following text is sent to all ISCAS complainants in England in order to establish that adjudication decisions will be shared with CQC: ***"ISCAS shares adjudication decisions with the Care Quality Commission (CQC), the regulator of hospitals in England. Your details will be anonymised, but the hospital/organisation will be identified. The CQC considers issues arising from complaints as part of the repository of information it holds on each hospital/organisation and may use this to recommend improvements."***

Where personal data (including sensitive personal data and/or confidential personal information) or identifiable information of people who use/used health and social care services (including their families or carers) is to be disclosed, this schedule must be approved by the CQC Caldicott Guardian prior to sign-off.

Signed off by:

Tom Ward
Care Quality Commission

19 November 2018

Sally Taber
Independent Sector Complaints Adjudication Service

20 November 2018

(The signatories have authorisation to make changes to the ISA on behalf of their organisation)