



IBIS Patient Data Procedure

Contents

1	Scope	2
2	Procedure	3
3	Definitions	7
4	Responsibilities	8
5	Audit and Review (evaluating effectiveness)	8
6	Equality Analysis	9
	Appendix A: IBIS Case Management Data Set	10
	Appendix B: Falls Notification Data Set	10
	Appendix C: Hypoglycaemic Notification Data Set	11
	Appendix D: GP Clinical Summary Data Set	12
	Appendix E: End of Episode Summary Data Set	12
	Appendix F: Blank ISP Template for External Agencies Using IBIS	13
	Appendix G: Patient Advice Leaflet	41



1

Scope

- 1.1. This document describes the use of IBIS (Intelligence Based Information System) within South East Coast Ambulance Service NHS Foundation Trust (The Trust), and provides information on the collection, storage, and retention of data.
- 1.2. The document also describes the transmission of patient identifiable data from the IBIS system.
- 1.3. IBIS is a system designed to assist with promoting an appropriate disposition for as many patients as possible. Disposition refers to the decision to convey, refer or discharge patients attended. Having more information about patients makes this process more effective and safer.
 - 1.3.1. Staff must follow the advice and guidance in the **Referrals Procedure** and **Discharge Procedure** where a patient does not require transport to hospital.
- 1.4. This document sits under the **Patient Data and Health Records Policy** and should be read in the context of the principles in that document.
- 1.5. **The aims of this procedure are:**
 - 1.5.1. To provide information on the use of IBIS and how it stores and uses patient information.
 - 1.5.2. To set out how data held on IBIS is managed and stored.
- 1.6. **The objectives of this procedure are:**
 - 1.6.1. To provide the organisation with understanding of the different functions of IBIS, and the implications for stored patient data which includes:
 - 1.6.1.1. Patient Case Management
 - 1.6.1.2. IBIS on iPad
 - 1.6.1.3. Falls Referrals and Notifications
 - 1.6.1.4. Hypoglycaemic Notifications
 - 1.6.1.5. GP Clinical Summaries
 - 1.6.1.6. End of Episode Summaries
 - 1.6.1.7. Explain the movement of data within IBIS
 - 1.6.1.8. To ensure IBIS users understand the implications for patient data when using the system operationally.



2 Procedure

2.1. Explanation of IBIS functions and data requirements

2.1.1. Patient Case Management

2.1.1.1. Patient Case Management is the storage of data about patients with complex or long-term health conditions who may be at risk of calling 999 or accessing '999 services' through NHS111.

2.1.1.2. Data is supplied by the patient's care team (for example community, primary, acute or social care) and provides a brief overview of the patient's ongoing needs should they access services from SECAMB in relation to their long-term health conditions.

2.1.1.3. The Trust does not case manage individual patients. Responsibility for the ongoing care of a patient is with their health or social care professional, or primary care team in the community.

2.1.1.4. Patient Care Plans are uploaded onto IBIS by the Patient Case Manager (PCM). The PCM is responsible for updating and managing the patient's care plan.

2.1.1.5. In the event of a 999 or 111 call, a process is undertaken to 'match' the IBIS record to the incident/case using initially a postcode or telephone number level match. Matching may also be undertaken using the patient's NHS Number, which can be obtained through the Personal Demographics Service (PDS).

2.1.1.6. *Please see appendix 1 for data sets.*

2.1.2. End of Episode Summaries

2.1.2.1. After an encounter with a patient that has an IBIS care plan in place, the system automatically produces an End of Episode Summary.

2.1.2.2. This summary is automatically sent out to the Patient Case Manager and/or the care team. There is also an option to send a copy of the End-of-Episode Summary to the patient's GP.

2.1.2.3. The summary contains information about the 999/111 call and can contain any extra information that the attending clinicians add to the 'clinical notes' section on IBIS.

2.1.2.4. *Please see appendix 5 for data sets.*



2.1.3. Falls Referrals and Notifications

- 2.1.3.1. If a Trust clinician identifies a patient who has fallen, they should seek consent from the patient to screen them through the Falls Risk Assessment Tool (FRAT) on IBIS. This will generate a Priority 1 or Priority 2 referral, or Priority 3 Notification, that is sent to a community-based Falls Prevention Service, Rapid Response Team and/or the patient's GP.
- 2.1.3.2. To be eligible for falls screening through IBIS the patient must be aged 65 years or over, non-conveyed and give consent.
- 2.1.3.3. If it is decided that a Falls Referral/Notification is appropriate, the attending SECamb clinician can screen the patient through the FRAT on IBIS using their Trust iPad.
- 2.1.3.4. For priority 1 and 2 referrals, the Trust have a Memorandum of Understanding (MoU) in place with the receiving community team that details a handover of patient care for further investigation and management.
- 2.1.3.5. A priority 3 notification is not a formal referral*. Rather it provides early warning to avoid subsequent falls by allowing the falls services to analyse the information passed from IBIS.
- 2.1.3.6. In the event that a SECamb clinician cannot access IBIS on their iPad, for example due to a lack of signal, then the clinician can contact the 'IBIS Desk' in EOC for completion over the phone or APP Hubs via eCal.
- 2.1.3.7. *Please refer to the **Referral, Conveyance and Discharge Policy** for the definitions of referral and discharge.
- 2.1.3.8. After data input by the attending clinician or the IBIS Data Assistant, the falls pro-forma is automatically turned into a PDF and sent by secure NHS.net email to the falls service and/or GP.
- 2.1.3.9. *Please see appendix 2 for data sets.*

2.1.4. Hypoglycaemia Notifications

- 2.1.4.1. If a Trust clinician identifies a patient who has had a hypoglycaemic episode, they should complete a hypoglycaemia notification on IBIS. This will generate a notification that is sent to a community-based Diabetes Service and/or the patient's GP.
- 2.1.4.2. To be eligible for a hypoglycaemia notification through IBIS the patient must have a treated hypoglycaemic episode and be non-conveyed. Notifications can be completed for patients of any age. The patient does not need to give consent for a hypoglycaemia notification to be completed.



- 2.1.4.3. If it is decided that a notification is appropriate, then the attending SECAmb clinician can complete a hypoglycaemia notification on their Trust iPad.
- 2.1.4.4. A hypoglycaemia notification is not a formal referral*. Rather it provides early warning to avoid subsequent hypoglycaemic episodes by allowing the diabetes services to analyse the information passed from IBIS.
- 2.1.4.5. In the event that a SECAmb clinician cannot access IBIS on their iPad, for example due to a lack of signal, then the clinician can contact the IBIS Desk in EOC for completion over the phone or via the APP Hubs via eCal.
- 2.1.4.6. *Please refer to the **Referral, Conveyance and Discharge Policy** for the definitions of referral and discharge.
- 2.1.4.7. After data input by the attending clinician or the IBIS Data Assistant, the hypoglycaemia pro-forma is automatically turned into a PDF and sent by secure NHS.net email to the diabetes service provider.
- 2.1.4.8. *Please see appendix 3 for data sets.*
- 2.1.5. **GP Clinical Summaries**
 - 2.1.5.1. Paramedic grade clinicians, and above, can use IBIS to send clinical summaries to GPs in Primary Care about their patients.
 - 2.1.5.2. Similar to falls and hypoglycaemia, this process is part of the documenting process and involves completing a pro-forma which is turned into a PDF and sent securely to the GP practice.
 - 2.1.5.3. The data is entered by the IBIS user, either attending clinician or IBIS Data Assistant and the information is sent automatically in electronic format to the patients GP practice via the Docman Connect service.
 - 2.1.5.4. *Please see appendix 4 for data sets.*
- 2.1.6. **IBIS on iPad**
 - 2.1.6.1. IBIS is accessible to front-line staff who have a personal issue Trust iPad. This allows staff to utilise IBIS functionality whilst on scene, at the patient's side.
 - 2.1.6.2. The attending SECAmb clinicians are alerted to the presence of patient information on IBIS via the Mobile Data Terminal (MDT) in the ambulance vehicle.
 - 2.1.6.3. Access to IBIS by SECAmb front line staff via their Trust-issued iPad is through a Mobile Data Management (MDM) Airwatch Browser. The browser provides an encrypted tunnel to the N3 network. Only crews assigned to the incident can view Patient Care Plans, which is audited.



2.1.7. Tracking of data in IBIS

- 2.1.7.1. All IBIS derived data is held within the Trust's secure data centre.
- 2.1.7.2. All individual records can be tracked and traced according to originating user and organisation.

2.1.8. Retrieval of data (in operational use and relating to data requests)

- 2.1.8.1. Data relating to care plans provided by external users can only be accessed when linked to an active 999/111 call. There is a matching process which has a staged approach to releasing data to ensure that the data is only accessed once the relationship with the patient has been confirmed and therefore legitimised.
- 2.1.8.2. Other data stored in the system can only be retrieved for reporting purposes in a redacted or anonymised way.
- 2.1.8.3. There is no system for looking up data prospectively within the patient case management function.
- 2.1.8.4. Incidents which have been attended can be accessed through other systems in keeping with current Trust processes for accessing patient data. Specifically, collating of data to identify frequent callers is a use of the data collected, and staff must obtain consent to pass data into IBIS.

2.1.9. Retention of IBIS data

- 2.1.9.1. All data on IBIS is retained according to the **Health Records and Patient Data Policy** and the **Health Records and Patient Data Management Procedures** in relation to retention periods.

2.1.10. Export of data

- 2.1.10.1. IBIS data can be exported under carefully controlled circumstances to "urgent care clinical dashboards" or other predictive analytics tool owned by Clinical Commissioning Groups.
- 2.1.10.2. There are specific governance processes which relate to this level of data sharing and the Trust will not export data without robust discussion, agreement and signatory of appropriate governance protocols.

2.2. Duties and responsibilities

- 2.2.1. IBIS requires data entry by Trust staff and external users, and this must be done accurately, following the principles in the **ePCR procedure** in relation to accurate completion.



2.2.2. For external IBIS users, there is an Information Sharing Agreement (ISA) which specifically states the data requirements, including accuracy and the need for contemporaneous record keeping. *Please refer to appendix 6.*

2.3. **Data security and legal obligations that apply to patient data**

2.3.1. The Trust is legally obliged to safeguard patient identifiable data, and only share data in the presence of consent (or as a best interest decision in the absence of capacity to consent).

2.3.2. Information must be kept secure at all times and staff must ensure that access to information is obtained through the compromise of the security systems which exist.

2.3.3. Please refer to the Health Records and Patient Data Policy for comprehensive advice and references to the essential documents which inform information security.

2.4. **Creation of IBIS records (all functions)**

2.4.1. IBIS records are created in one of two ways; data entry by a Patient Case Manager, and data entry by Trust employees during completion of the “coding” part of the system for referrals/notifications.

2.4.2. Coding for referrals/notifications can be undertaken by eligible Trust staff either through IBIS on iPad or on Trust PC computers, and this is accessed via the usual Trust security login procedure.

2.4.3. Patient Case Management records are entered via a secure web-based form, accessed by the user via a secure login process. All activity on IBIS is recorded in a log-file database which is retained according to the Trust’s Information Governance Policy.

2.4.4. In no circumstances is patient data retained on a local computer. All data is stored “server-side”.

2.4.5. Web forms for external users time-out after 15 minutes to minimise the risk of an account being compromised should the user forget to end a work session.

3 **Definitions**

3.1. IBIS – Intelligence Based Information System

3.2. EOC – Emergency Operations Centre (ambulance control)

3.3. PCM – Patient Case Manager



4 Responsibilities

- 4.1. The **Chief Executive Officer** has ultimate responsibility for this procedure.
- 4.2. The **Senior Clinical Operations Manager** is responsible for managing the procedure, as well as monitoring and auditing.
- 4.3. **All Operational staff** are responsible for following the procedure, regardless of the environment in which IBIS is utilised or accessed.

5 Audit and Review (evaluating effectiveness)

- 5.1. All procedures have their effectiveness audited by the responsible Management Group at regular intervals, and initially six months after a new policy is approved and disseminated.
- 5.2. Effectiveness will be reviewed using the tools set out in the Trust's Policy and Procedure for the Development and Management of Trust Policies and Procedures (also known as the Policy on Policies).
- 5.3. This document will be reviewed in its entirety every three years or sooner if new legislation, codes of practice or national standards are introduced, or if feedback from employees indicates that the policy is not working effectively.
- 5.4. All changes made to this procedure will go through the governance route for development and approval as set out in the Policy on Policies.
- 5.5. The **IBIS Lead Manager** will be responsible for ensuring adherence to the procedure by reviewing internal reporting systems (e.g. risk registers).
- 5.6. Any non-compliance or deviation from this procedure that results in an adverse outcome for a patient will be dealt with in accordance with the Incident Reporting Manual and referred to the Professional Standards Department.
 - 5.6.1. All staff and managers are responsible for reporting incidences of practice operating outside the definitions laid out in this document.
 - 5.6.2. Reporting will be done through the usual Trust systems of incident reporting, such as:
 - 5.6.2.1. Patient Experience Team (PET)
 - 5.6.2.2. Datix Incident Form (DIF1) report forms
 - 5.6.2.3. Serious Incidents (SI) report



Equality Analysis

The Trust believes in fairness and equality, and values diversity in its role as both a provider of services and as an employer. The Trust aims to provide accessible services that respect the needs of each individual and exclude no-one. It is committed to comply with the Human Rights Act and to meeting the Equality Act 2010, which identifies the following nine protected characteristics: Age, Disability, Race, Religion and Belief, Gender Reassignment, Sexual Orientation, Sex, Marriage and Civil Partnership and Pregnancy and Maternity.

Compliance with the Public Sector Equality Duty: If a contractor carries out functions of a public nature then for the duration of the contract, the contractor or supplier would itself be considered a public authority and have the duty to comply with the equalities duties when carrying out those functions.



Appendix A: IBIS Case Management Data Set

First Name	Last Name	Known As	Date of Birth
Gender	NHS Number	Telephone Number	Multi-occupancy address
House name/number	Street address	Postcode	GP practice
Consent level given	Allergies	Clinical History and Associated Risks	Clinical Instructions
DNACPR Status	Preferred Place of Care	Preferred Place of Death	Long term conditions (multi-select list)

Appendix B: Falls Notification Data Set

Patient's Full Name	Age	Date of Birth	Sex
Address	Telephone number	Next of kin and contact details	Property type
Patient consent	NHS Number	Date form completed	Incident Number
Patient's GP	Patient's GP surgery	Type of fall	Narrative of fall
Condition code	Care provided	Has the patient fallen two or more times in the last 6 months?	Has the patient suffered more than one fall in the last 3 days?
Does the patient take 4 or more medicines per day?	Has the patient been taking any Benzodiazepines (tranquillisers, sleeping tablets etc.) for more than 2 weeks?	Has the patient been suffering new giddiness within the last week – on standing or sitting up in bed?	Has the patient experienced any recent deterioration with their eyesight and/or wear bi-focals?
Does the patient have problems with their hearing?	Does the patient appear unsteady when walking (shuffling or taking uneven steps)?	Does the patient hold onto furniture or walls when they walk?	Does the accommodation appear to have any slip/trip hazards?



Do you believe the patient need assessment for handrails or appliances?	Does the patient suffer from any of the following: Social Isolation, Alcohol Problems, Self-Neglect, Depression, Malnutrition, Fear of Falling	Does the patient have a diagnosis of Parkinson's or Stroke?	NHS Foundation Trust Does the patient struggle to get up from a chair at knee height without using their hands?
Notes:	Requested by, (Crew name)	Call Sign	Form Completed by

Appendix C: Hypoglycaemic Notification Data Set

Patient's full name	Age	Date of Birth	Sex
Patient's address	Patient's telephone number	Next of kin and contact details	Property type
Patient's consent	NHS number	Date form completed	Incident number
Patient's GP	Patient's GP surgery	Blood glucose (BM) on arrival (pre-treatment)	Blood glucose (BM) post treatment
Was third party assistance (SECAmb, family, bystander) required to resolve this hypoglycaemic episode?	Likely reason for onset of hypoglycaemia (precipitating factors) – select all that apply	Is the patient aware of how to self-manage?	Does the patient object to information being shared with GP?
Patient medical history	Any further information the crew would like to pass on	Requested by (crew name)	Call sign



Appendix D: GP Clinical Summary Data Set

Incident number	Date/time of incident	Problem	History
Examination	Impression	Treatments	Outcome code
Suggested Follow-up	Clinician	Prepared by	

Appendix E: End of Episode Summary Data Set

SECAmb incident number	Date and time report produced	NHS Number	Patient's name
Surgery	Case Manager	Care team	CCG Code
Date of 999 call	Conveyance/Non-Conveyance	Hospital arrival time	Episodes (number)
Previous conveyances (number)	Incident address	Call source	Cancel/closed reason
Problem/condition	Time of patient match	IBIS clinician	IBIS notes
IBIS end of episode reason			



Information Sharing Protocol

between

South East Coast Ambulance Service
NHS Foundation Trust

and

[Organisation]



Acronyms and Definition of Terms.....	4
1. Introduction.....	9
2. What is Information Sharing.....	9
3. Purpose.....	10
4. Terms of Agreement.....	10
5. Legislation and Guidance.....	11
6. Key Information Sharing Advisory and Support Roles.....	11
7. Organisational Responsibilities.....	15
8. Conditions for Processing.....	15
9. Review of this Protocol.....	20
10. Endorsement	20
11. Signatory Organisations.....	20

Appendix 1: Legislation and Guidance

Appendix 2: Information Sharing Protocol Sign-Up Sheet

This ISP is not a licence to share information but a guide that must be followed by all staff planning to share information between organisations. It provides a set of guiding principles and gives assurance that there is a consistent approach across the footprint in relation to information sharing

1. Introduction

This Information Sharing Protocol (ISP) seeks to improve the manner in which Personal and Special Categories of Data, as defined in the EU General Data Protection Regulation 2018 / Data Protection Act 2018, is shared between [Organisation] and South East Ambulance Service NHS Foundation Trust (SECAMB).

SECAMB's Intelligence Based Information System (IBIS) is a communication tool that links the Ambulance Service to wider Health and Social care systems. It is designed to enable ambulance clinicians to have up to date information about a patient's health, their care plans, their needs and wishes.

It also allows the ambulance service to play an integral part in the pro-active management and ongoing care of patients in partnership with community teams. Teams can use IBIS to monitor and manage their patients' 999 interactions, as well as use it as a foundation for Multidisciplinary Team (MDT) meetings.



IBIS has multiple features, including the ability to securely send referrals to community teams and clinical summaries to GPs, however this ISP only relates to the Patient Case Management (care plan sharing) functionality. It aims to provide guidance around information governance and risk together with the monitoring of compliance.

An IBIS Patient Data Procedure document is in place, which provides information on the collection, storage and retention of data. This document is found with the Trust's intranet and is accessible by all SECAmb staff.

This ISP comprises a set of rules that organisations agree to comply with when sharing Personal and Special Categories of Data, known collectively as Personal Confidential Data (PCD), as defined within the Definitions and Legislation Summaries set out within this agreement. This sets out the obligations and commitments that staff must follow to ensure that legislation is not breached, and patients'/ clients'/ families'/ carers'/ staff/ employees' confidentiality is maintained.

The General Data Protection Regulation, Data Protection Act 2018, Common Law Duty of Confidentiality, Human Rights Act 1998 and (to a certain extent) the Freedom of Information Act 2000 (FOI) play a major role in the use and protection of individual information.

2. Data Set of IBIS Records

The following data is supplied by the Patient Case Manager (PCM) for each IBIS record:

- First Name
- Surname/Last Name
- "Known as" (preferred name)
- Telephone number
- NHS Number
- Date of birth
- Gender
- House Name/Number
- Address
- Postcode
- Multi-occupancy property (check box)
- GP practice
- Consent level
- Allergies
- Clinical history and associated risks (e.g. past medical history, baseline observations)
- Clinical instructions (care plan and/or contingency information)
- DNACPR status (none/active/withdrawn)
- Advanced care plan in place (none/active/withdrawn)
- Preferred Place of Care
- Preferred Place of Death
- Medical conditions (multi-select from list)
- Contact information for case managers



Patient Case Managers can also upload documents to accompany the data entered into the system. Any uploaded documents will be considered as part of the care record and be retained and disposed of accordingly.

3. What is Information Sharing

Information Sharing is the disclosure, exchange or pooling of personal information between organisations acting as Data Controllers in their own right and for their own purposes. This may include routine sharing of datasets used to plan and improve services or 'ad hoc' disclosures that support or protect individuals. Information may be shared for more than one purpose.

The terms 'Information Sharing' and 'Data Sharing' refer to sharing for either Direct Care or Secondary Uses.

People expect organisations to share their Personal Confidential Data (PCD) where it helps to provide or improve the services they need. It is part of the way local health and social care services work and should be approached with confidence.

This ISP sets out principles for respecting the privacy and confidentiality of individuals, protecting their PCD whilst ensuring they receive effective and efficient services.

4. Consent

Direct Care

The legal gateway for sharing Special Categories of Data for this purpose under GDPR is covered in Article 9, that the:

[P]rocessing 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 or pursuant to contract with a health professional [...].

For this to be achieved a gateway from Article 6 also need to have been satisfied, that:

[P]rocessing is necessary for the performance of a task carried out in the public interest or on the exercise of official authority vested in the controller.

On this basis consent to process is not generally required under GDPR for the provision of Direct Care. However, practitioners (both IG and clinical) must maintain an awareness of the Common Law Duty of Confidentiality, that is law created by judicial precedent rather than Act of Parliament which codifies that information confided should not be used or disclosed further, except as originally understood by the confider, or with their subsequent permission.

If neither implied nor explicit consent has been obtained to further share information, it is beholden on the Data Controller (or their operative, the member of staff) to make an appropriate decision to share, basing it on whether disclosure is essential to



safeguard either the Data Subject or a third party and it is considered to be in the public interest. There may also be a legal obligation to share the information, such as a Court Order, although this would be covered by another GDPR Condition for Processing.

Any objection to sharing information will be noted on the respective organisations clinical system and information will not then be shared with SECAmb

5. Purpose

This ISP applies generally to the sharing of information, which involves PCD. It provides a framework within South East Coast Ambulance Service and Sussex Partnership NHS Foundation Trust for the secure sharing of individual information with South East Coast Ambulance Service in a manner compliant with statutory, regulatory and professional responsibilities.

South East Coast Ambulance Service and Sussex Partnership NHS Foundation Trust shall be the joint Data Controllers in common in respect of all data processing activities in relation to Trust Data. Its purpose is to ensure that everyone understands:

- ✓ The importance of Information Sharing, where it improves care for individuals, enhances the efficiency and performance of organisations and where the information sharing is for the direct continuing care of users of service.
- ✓ That only the minimum information necessary for the purpose should be shared.
- ✓ That when it is necessary to share, it complies with the law, guidance and best practice.
- ✓ That individuals' rights must be respected, particularly confidentiality and security.
- ✓ That confidentiality must be adhered to unless there is a robust public interest or a legal justification in disclosure.
- ✓ The importance and benefits of information security and confidentiality training.
- ✓ The ramifications of the seventh Caldicott Principle, that the duty to share information can be as important as the duty to protect patient confidentiality.

6. Terms of Agreement

This ISP must be used by any authorised team which sits within **[Organisation]**. In doing so, any signatories agree to be bound by the authorised teams:

- a. In signing this ISP you are confirming that you are authorised to enter into agreements on behalf of your organisation and that your organisation's processing activities are carried out in accordance with Article 30 of the General Data Protection Regulations (GDPR).
- b. Parties to this ISP are responsible for the ongoing protection and lifecycle management of personal information received unless otherwise agreed in writing
- c. This ISP should not be used to govern disclosure of personal information to a service provider acting solely under the instruction of the Data Controllers.
- d. The GDPR defines these as Data Processors. Such arrangements are accountable through contracts or service agreements that include appropriate data protection clauses.



Only signatories to this ISP are bound by its terms, however it can be advocated that individual parties (e.g. teams) with whom information is shared sign in their own right.

- f. Disclosures made under this agreement do not transfer copyright ownership or intellectual property rights unless expressly stated otherwise or appropriately licensed.
- g. Parties to this agreement must each nominate an Information Governance (IG) Lead/Manager to act as that organisation's point of contact.
- h. A sending (disclosing) party is responsible for ensuring that outbound personal information is appropriately protected in transit. Responsibility for protection transfers to the recipient organisation once accessed or opened by that organisation or one of its employees, contractors or agents.

7. Organisational Responsibilities

This ISP provides a framework for all authorised Health & Social Care teams within **[Organisation]** for the secure sharing of individual information with South East Coast Ambulance Service in a manner compliant with statutory and professional responsibilities.

Organisations and teams undertake to:

- Implement and adhere to this ISP
- Ensure that all protocols and procedures established within the respective organisation(s) are consistent with this ISP.
- Establish systems, raise awareness, inform individuals, issue specific guidance and provide training to their staff to ensure compliance with this ISP
- Ensure all staff working within their own organisations have access to this document and they are aware how to use it and who to go to for more detailed information and/or guidance when dealing with information requests/sharing.

7.1 Security of Information being shared

There is an absolute requirement for **[Organisation]** and SECAMB to hold information securely. SECAMB is responsible for the security of all electronically stored records held on IBIS. All record storage is done electronically, this is on a secure encrypted computer and accessible only to those individuals who have a legitimate business need. No hard copies of IBIS patient records are stored by SECAMB.

The information shared must not be disclosed to any third party without the written consent of the service user; unless it is disclosed under a statutory obligation, for example as a result of a Court ordering disclosure.

[Organisation] and SECAMB undertake to ensure that they will collect, process, store, disclose and dispose of all information held within the terms of this agreement, and the relevant legislation. **[Organisation]** and SECAMB agree that they will ensure that all information held is accurate, relevant and fit for the purpose for which it is intended. Appropriate technical and organisational measures shall be taken by **[Organisation]** and SECAMB against unauthorised or unlawful processing of information and against accidental loss or destruction or damage to information.

7.2 Information Governance Training



IG awareness and mandatory training procedures must be in place in all Health & Social Care organisations so that all staff, including new starters, locums, temporary, students, volunteers, peer mentors and staff contracted to work in their respective organisations are appropriately trained on an annual basis.

To this end, an IG training programme must be developed which includes a Staff Training Needs Analysis, induction for new starters and the completion of basic IG training on an annual basis with an individual test of comprehension by all staff.

7.3 Retention and Disposal

Personal information disclosed under this ISP will not be held for longer than necessary to fulfil the purpose for which it was collected and will be disposed of securely in accordance with national guidance and each organisation's local information retention and disposal policy.

This information will only be accessible by appropriate personnel and will be retained in accordance with national standards as set out within the IGA NHS Records Management Code of Practice 2016.

7.4 Subject Access and Freedom of Information Requests

Participating partner organisations acknowledge a duty to assist one another in meeting their individual responsibilities under the General Data Protection Regulation / Data Protection Act 2018 and the Freedom of Information Act 2000 to provide information subject to this agreement in response to formal requests.

7.5 Breach of Agreement

Any breach of this protocol must be reported and investigated in line with each partner organisation's incident reporting, management procedure, and any relevant statutory guidance.

7.6 Complaints

Each partner organisation has a formal procedure by which individuals can direct, their complaints regarding the application of this information sharing agreement

8. Review of this Protocol

This ISP will be reviewed bi-annually or sooner if legislation or service changes dictates. A review will be undertaken by each partner organisation under the programme whose IG Working Groups will ratify the protocol for use.

9. Endorsement

This document has been drafted by South East Coast Ambulance Service and [Organisation] and is endorsed by an appropriate representative (e.g. Chief Executive, Caldicott Guardian, SIRO and Data Protection Officer) of the signatory organisations.



Signatory Organisations

Signing and returning the sign-up sheet in **Appendix 2** indicates that the signatory confirms acceptance of the terms and principles of the South East Coast Ambulance NHS Foundation Trust Information Sharing Protocol on behalf of their employing organisation.

A schedule of ISPs is maintained by the Information Governance Lead within South East Coast Ambulance Service NHS Foundation Trust.



Appendix 1: Legislation and Guidance

South East Coast Ambulance Service



NHS Foundation Trust

The main pieces of legislation guiding and supporting Information Sharing include, but are not necessarily limited to:

- Access to Health Records Act 1990
- Civil Contingencies Act 2004
- Freedom of Information Act 2000
- General Data Protection Regulation 2016
- Health and Social Care Act 2012
- Health and Social Care (Safety and Quality) Act 2015
- Human Rights Act 1998
- Mental Capacity Act 2005
- Equality Act 2010
- Privacy and Electronic Communications Regulations 2003

Legislation restricting the sharing of information only between the Health & Social Care professionals caring for the individual include:

- Abortion Act 1967
- Adoption Act 1976
- Gender Recognition Act 2004
- Human Fertilisation and Embryology (Disclosure of Information) Act 1992
- Venereal Diseases Act 1917
- Venereal Diseases Regulations of 1974 and 1992

In addition to legislation, there is a multitude of guidance, which is generally considered highly advisory, if not binding, on the Health & Social Care services and providers, including, but not necessarily limited to:

- [A Manual for Caldicott Guardians](#) (UK Caldicott Guardian Council, 2017)
- [Anonymisation: Managing Data Protection Risk Code of Practice](#) (ICO, 2012)
- [Confidentiality NHS Code of Practice](#) (DoH, 2003)
- [Information: To Share or Not to Share](#) (a.k.a. *Caldicott2*), including the reviewed Caldicott Principles (Independent IG Oversight Panel, 2013)
- [Records Management Code of Practice for Health and Social Care](#) (IG Alliance, 2016)
- [Report on the Review of Patient-Identifiable Information](#) (a.k.a. *The Caldicott Report*), including the original Caldicott Principles (DoH, 1997)
- [Review of Data Security, Consent and Opt-Outs](#) (a.k.a. *Caldicott3*) (National Data Guardian, 2016)
- [Safe Data, Safe Care Report](#) (Care Quality Commission, 2016)

Furthermore, there are various good practice guidelines concerning Information and Cyber Security including, but not necessarily limited to:

- [ISO 27001:2013, International Information Security Management System Standard](#)



Each organisation has management roles to assist with sharing of personal information. These roles are listed and detailed below. All training given to staff should ensure it includes this information.

12. Data Protection Officer

The only legislative role for public authorities with regard to Information Sharing is the Data Protection Officer (DPO), as outlined in the GDPR.¹ Key tasks of the role include:

- Informing and advising people and organisations who process information on behalf of the organisation of their Data Protection obligations.
- Monitor compliance with the Data Protection provisions, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits.
- Provide advice on the completion of Data Protection Impact Assessments (DPIA).
- Cooperate with the Information Commissioner's Office (ICO), and acting as the contact point with it on issues relating to processing.
- Having due regard to the risks associated with processing operations, taking into account the nature, scope, context and purposes of processing.

As joint data controllers, each data controller is responsible for providing assurance when performing its own data processing activities and must::

- Ensure that the DPO is fully involved in a timely manner in all Data Protection issues.
- Support the DPO in performing their tasks by providing resources necessary to complete them, as well as access to Personal Data and processing operations, and maintaining their expert Data Protection knowledge.
- Ensure that the DPO does not receive any instructions regarding the exercise of those tasks. The DPO cannot be dismissed or penalised for performing their tasks.²
- Report to the highest management level of the Data Controller or Data Processor.

In addition:

¹ GDPR Articles 37-39.

² GDPR Article 38(3).



Data Subjects may contact the DPO with regard to all issues related to processing of their Personal Data and to the exercise of their rights under the GDPR. The DPO shall be bound by secrecy or confidentiality concerning the performance of their tasks, in accordance with Union or Member State law.

South East Coast Ambulance Service NHS

NHS Foundation Trust

Depending on the structure of the respective organisation, the DPO may or may not be the IG Head/Lead/Manager, depending on the structure of the respective organisation.

13. Senior Information Risk Owner

The Department of Health's (DoH) 2017 guidance³ is that the Senior Information Risk Owner (SIRO):

- Must be an Executive Director or other senior member of the Board (or equivalent senior management group/committee). The SIRO may also be the Chief Information Officer (CIO) if the latter is on the Board, but should not be the Caldicott Guardian as the SIRO should be part of the organisation's management hierarchy rather than being in an advisory role.
- Will be expected to understand how the strategic business goals of the organisation may be impacted by information risks and it may therefore be logical for this role to be assigned to a Board member already leading on risk management or IG.
- Will act as an advocate for information risk on the Board and in internal discussions, and will provide written advice to the Accounting Officer on the content of the annual Statement of Internal Control (SIC) in regard to information risk.
- Will provide an essential role in ensuring that identified information security risks are followed up and incidents managed and should have ownership of the Information Risk Policy and associated risk management Strategy and processes. He/she will provide leadership and guidance to a number of Information Asset Owners.
- Has key responsibilities to:
 - Oversee the development of an Information Risk Policy, and a Strategy for implementing the policy within the existing IG Framework.
 - Take ownership of the risk assessment process for information and cyber security risk, including review of an annual information risk assessment to support and inform the SIC.
 - Review and agree action in respect of identified information risks.

³ Information Governance Toolkit, Acute Type, v14.1, Requirement 307 (see <https://www.igt.hscic.gov.uk/RequirementQuestionNew.aspx?tk=429253737175266&Inv=2&cb=a620c60b-cbaf-4584-a2cc-83250509e1e1&sViewOrgType=2&reqid=3036>).



- Ensure that the organisation's approach to information risk is effective in terms of resource, commitment and execution and that this is communicated to all staff.
- Provide a focal point for the resolution and/or discussion of information risk issues.
- Ensure the Board is adequately briefed on information risk issues.
- Ensure that all care systems Information Assets have an assigned Information Asset Owner.

13.1 Caldicott Guardian

The UK Caldicott Guardian Council's 2017 guidance is that the Caldicott Guardian must:

- Be a senior person within a health or social care organisation.
- Makes sure that the personal information about those who use its services is used legally, ethically and appropriately, and that confidentiality is maintained.
- Be able to provide leadership and informed guidance on complex matters involving confidentiality and information sharing.
- Play a key role in ensuring that their organisation satisfies the highest practical standards for handling person-identifiable information.
- Retain as their key concern is information relating to patients, service users and their care, but be mindful that the need for confidentiality extends to other individuals, including their relatives, staff and others.
- Apply the seven Caldicott principles wisely, using common sense and an understanding of the law.
- Be compassionate, recognising that their decisions will affect real people, some of whom they may never meet.
- Be mindful that the importance of the Caldicott Guardian acting as “the conscience of the organisation” remains central to trusting the impartiality and independence of their advice.

13.2 Information Governance Lead / Head of Information Governance

The IG Lead / Head of Information Governance for each organisation supports the Caldicott Guardian and SIRO with IG, security and confidentiality issues related to the sharing of PCD. This includes regular IG Working / Steering Group meetings DoHs 2017 guidance⁴ is that they must be a representative from the senior level of management who co-ordinates the IG work programme.

⁴ Information Governance Toolkit, Acute Type, v14.1, Requirement 307 (see <https://www.igt.hscic.gov.uk/RequirementQuestionNew.aspx?tk=429254877817166&Inv=2&cb=70606326-5ba1-438b-b29d-693ec1d96d60&sViewOrgType=2&reqid=2965&first=true>).



They are accountable for ensuring effective management, accountability, compliance and assurance for all aspects of IG and have the following key tasks:


- Developing and maintaining the currency of comprehensive and appropriate documentation that demonstrates commitment to and ownership of IG responsibilities, e.g. an over-arching high-level strategy document supported by corporate and / or directorate policies and procedures.
- Ensuring that there is top-level awareness and support for IG resourcing and implementation of improvements.
- Providing direction in formulating, establishing and promoting IG policies.
- Establishing working groups, if necessary, to co-ordinate the activities of staff given IG responsibilities and progress initiatives.
- Ensuring annual assessments using the IG Toolkit (and its successor framework) and audits of IG policies and arrangements are carried out, documented and reported in line with the requirements of the NHS Standard Contract.
- Ensuring that the annual assessment and improvement plans are prepared for approval by the senior level of management, e.g. the Board or senior management team, in a timely manner. For example, for NHS Trusts sign off may be scheduled in advance of the end of financial year submission on the 31 March each year.
- Ensuring that the approach to information handling is communicated to all staff and made available to the public.
- Ensuring all IG staff understand the need to support the safe sharing of PCD for Direct Care as well as the need to protect individuals' confidentiality;
- Ensuring that appropriate training is made available to all staff and completed as necessary to support their duties.
- Liaising with other committees, working groups and programme boards in order to promote and integrate IG standards.
- Monitoring information handling activities to ensure compliance with law and guidance;
- Providing a focal point for the resolution and/or discussion of IG issues.

14. Information Asset Owners

DoH's 2017 guidance⁵ is that organisations have Information Asset Owners (IAO), with the following role:

- For Information Risk, they are directly accountable to the SIRO and will provide assurance that Information Risk is being managed effectively for their assigned Information Assets. In large organisations IAOs may be assisted in their roles by
-



staff acting as Information Asset Administrators who have day to day responsibility for management of information risks affecting one or more assets. 

- It is particularly important that each IAO should be aware of what information is held, and the nature of and justification for Data Flows to and from the Information Assets for which they are responsible.
- The role of the IAO is to understand what information is held, what is added and what is removed, how information is moved, who has access and why. As a result, they should be able to understand and address risks to the information and to ensure that information is fully used within the law for the public good. The IAO will also be responsible for providing or informing regular written reports to the SIRO, a minimum of annually on the assurance and usage of their asset.
- It is important that “ownership” of Information Assets is linked to a post, rather than a named individual, to ensure that responsibilities for the asset are passed on, should the individual leave the organisation or change jobs within it.
- It is the responsibility of IAOs to ensure there is good understanding of the hardware and software composition of their assigned assets to ensure their continuing operational effectiveness. This includes establishing and maintaining asset records that will help predict when asset configuration changes may be necessary.

15. Conditions for Processing

Health & Social Care services share information about service users for the purposes of Direct Care and for Secondary Uses beyond this.

16. Direct Care

The legal gateway for sharing Special Categories of Data for this purpose under GDPR is covered in Article 9, that the:

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 or pursuant to contract with a health professional [...].⁶

For this to be achieved a gateway from Article 6 also need to have been satisfied, that:

⁶ GDPR Article 9(2)(h).



Processing is necessary for the performance of a task carried out in the public interest or on the exercise of official authority vested in the controller.

South East Coast Ambulance Service NHS

NHS Foundation Trust

On this basis Consent to process is not generally required under GDPR for the provision of Direct Care. However, practitioners (both IG and clinical) must maintain an awareness of the Common Law Duty of Confidentiality, that is law created by judicial precedent rather than Act of Parliament which codifies that information confided should not be used or disclosed further, except as originally understood by the confider, or with their subsequent permission.⁸

Generally, if a Data Subject's Personal Confidential Data is disclosed in circumstances where it is expected that a duty of confidence apply, it should not normally be disclosed further without that Data Subject's consent. In Health & Social Care this Duty applies very strongly in the Service User / professional relationship.

Under GDPR the expectation is that information will be shared under the provision of 'Direct Health Care' purposes. Patients will be informed of how their information is shared and with whom through conversations with their clinician / care team and through the use of patient information leaflets and robust privacy notices. They can however choose to withhold the sharing of their clinical information although they must be informed of the potential risk / outcome of not doing so all of which must be noted within the clinical record.

If neither implied nor explicit consent has been obtained to further share information, it is beholden on the Data Controller (or their operative, the member of staff) to make an appropriate decision to share, basing it on whether disclosure is essential to safeguard either the Data Subject or a third party and it is considered to be in the public interest.

There may also be a legal obligation to share the information, such as a Court Order, although this would be covered by another GDPR Condition for Processing.

Despite having a legal basis for sharing information the individual / organisation retains a duty under Article 32(1) to ensure that the security of the information is not breached to anyone while it is being transferred between facilities.⁹ This means that for information in transit the Data Controller and / or Data Processor must implement appropriate technical

⁷ GDPR Article 6(1)(e).

⁸ Department of Health (2003), *Confidentiality NHS Code of Practice*, p.13.

⁹ GDPR Article 32.



and organisational measures to ensure a level of security appropriate to the risk, as appropriate, such as:

HS

- Pseudonymisation and encryption of Personal Data.
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.
- The ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident.
- A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

16.1 Secondary Uses

As with Direct Care, to allow such processing the organisation must ensure that at least one requirement each of GDPR Articles 6 and 9 are met.

To legally share Personal Data, at least one of the following Article 6 criteria must be met:

- The Data Subject has given consent to the processing for specific purposes.
- Processing is necessary for the performance of a contract to which the Data Subject is or will be party to.
- Processing is necessary for compliance with a legal obligation to which the Data Controller is subject.
- Processing is necessary in order to protect the vital interests of the Data Subject or another 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 Data Controller.

Furthermore, to share Special Categories of Data, at least one of the following Article 9 criteria must be met:

- 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 Data Controller or of 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 is carried out in the course of its legitimate activities with appropriate safeguards by a charity.
- Processing relates to Personal Data that has been 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, while respecting the fundamental rights and the interests of the Data Subject.
- 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.
- 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.
- Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance.

Where consent is used as the basis for processing, this is understood as any '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'.¹⁰

Generally, under the new Data Protection legislation consent is not required where there is another condition for processing.

In the specific case of sharing Personal Data for planning of services, the legal gateway is most likely to be the Article 9 clause that:

*[P]rocessing 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 which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy.*¹¹

¹⁰ GDPR Recital 32.

¹¹ GDPR Article 9(2)(i).



Similarly, many elements of healthcare planning may fall under the 'management of health and social care systems and services'. Organisations intending to use this criterion would need to assess whether or not it believes this allows cross-organisational sharing for secondary purposes.

The clause noted from Article 6 under 8.1, will also need to have been met before any of Article 9 can be.

It is likely that the potential need to share for Secondary Uses will require a DPIA to be completed, and this will be mandatory where identifiable Special Categories of Data are present. The template to be used is bespoke for each organisation. For DPIAs that are agreed, where the sharing is either large scale or to be undertaken on a regular / permanent basis, a standard Information Sharing Agreement will need to be put in place.



Anonymised information may be used without consent and requires the removal of.

South East Coast Ambulance Service **NHS**

NHS Foundation Trust

Name

Address

- Full postal code
- NHS number
- Date of birth
- Local Identifiers, e.g. hospitals numbers
- Anything else that could identify an individual e.g. photograph, x-ray, dental records.

Information that has been anonymised can never be reverted to its original form.

Similarly, pseudonymisation can be used, but this has the ability to be re-identified at a later point.

Information Sharing Protocol for Secondary Uses of Personal Confidential Data

For regular / permanent sharing of PCD for Secondary Uses where a DPIA has been signed off an ISA will need to be completed.

- What information is to be shared.
- The business rationale for sharing it.
- The legal basis for sharing it under GDPR Article 6 and 9 (as per Highlight Box 3).
- The benefits to either the:
 - Data Subject, or
 - Organisation, or
 - H&SC economy.
- Which organisation is the Data Controller.
- How Data Quality will be assured, going forward.
- What processes are in place to assure the Information Security of the processing:
 - When in transit from the sending to the receiving organisation, and / or
 - At the receiving organisation.
- What the arrangements are for the retention and disposal of the information.
- How requests concerning the use of the information under FOI will be managed between the organisations.
- How Data Breaches will be dealt within in line with the new Data Protection law.



- The date the protocol is effective from, and for how long.
- Sign-off by a responsible manager within the sending and receiving organisations.
- Sign-off from the Caldicott Guardian for the sending organisation.

16.2 Capacity

An individual may be unable to give consent if they:

- **Are a minor.** Although there is no clear guidance in UK law relating to what age defines a child, those that have the capacity and understanding to take decisions about their own care and treatment are also entitled to make decisions about the use and disclosure of information they have provided in confidence. Capacity is usually defined by the professional providing care, based on their professional judgement at that time, dependent upon the nature of the issue in question (Gillick/Fraser competency).
- Different levels of capacity may be required for different levels of decision making with regard to information sharing. If the healthcare professional treating the child does not believe the child has capacity, then the child's parent / guardian with parental responsibility will make the decision to share information or not. Where there is any doubt as to whether the decision to share information, made by those with parental responsibility, is in the child's best interests, the matter may need to be referred to the courts to decide.
- **Are unconscious.** In the individual's best interest, any decision to share information will be taken by the healthcare professional treating the individual at that time. The decision to share information must be justified and documented in the individual's record.
- **Do not have the mental capacity.** An individual may not have capacity to make specific decisions whether or not to share their PCD.

It is necessary to be aware of the guidance issued under the Mental Capacity Act 2005 (MCA). When deciding to share information belonging to those who do not have the mental capacity, H&SC professionals should take account of a variety of factors, such as sharing in the service user's best interests; the safety of staff caring for the individual, relatives of the individual and the public interest; the GDPR guidelines.

16.3 Best Interest

The Health and Social Care (Safety and Quality) Act 2015 places a duty on English H&SC providers and commissioners to share information when it is considered likely to facilitate the provision of care to an individual in their best interests. The duty does not apply where an individual objects, or would be likely to object, or where the information is connected with the provision of care by an anonymous access provider, such as a sexual health service, or where the duty cannot be reasonably complied with for other reasons. It does not override duties under the Common Law or the GDPR.

16.4 Information Held in Shared or Hosted Databases



All data owners (these may be data owners from many organisations) must be registered as one of a number of joint Data Controllers and each Data Controller will retain control over their own information. Organisations may give written authority delegating the 'assigning of access' to one Caldicott Guardian to act on their behalf, although the data owners will still be responsible and accountable for their own data.

The process may vary in different organisations but whichever system is used, the Caldicott Guardian should sign off all accesses to service-user identifiable information. Caldicott Guardians may find they are asked to allow various groups (e.g. analysts) access to the information held in the database for one of a number of purposes.

Caldicott Guardians must ensure the purposes are lawful and comply with the guidance contained in this document. Where the delegated Caldicott Guardian cannot make a judgment alone he/she should consult all Caldicott Guardians concerned and/or seek expert advice.

Definitions and Legislation Summaries

Access to Health Records Act 1990 This Act gives patients' representatives right of access to their held Medical Records, in respect of information recorded on or after 1 November 1991. It is only applicable for access to deceased persons' records. All other requests for access to information by living individuals are provided under the access provisions of domestic legislation based on the General Data Protection Regulation. The full Act is available on the government's [Legislation](#) website.

Caldicott Principles The principles, which guide and reflect good Data Protection practice in the health and social care sector, are:

1. Justify the purpose(s) for using confidential information
2. Don't use Personal Confidential Data unless it is absolutely necessary
3. Use the minimum necessary Personal Confidential Data
4. Access to Personal Confidential Data should be on a strict need-to-know basis
5. Everyone with access to Personal Confidential Data should be aware of their responsibilities
6. Comply with the law
7. The duty to share information can be as important as the duty to protect patient confidentiality



Care Act 2014

Under Act, Local Authorities have updated functions, to make sure people who live in their areas:

- Receive services that prevent their needs becoming more serious
- Receive information to make good decisions about care
- Have a range of quality services to choose from

The full Act is available on the government's [Legislation](#) website.

Civil Contingencies Act 2004

The Act has an overall objectives focused on the management of three types of threat:

- Serious damage to human welfare.
- Serious damage to the environment.
- War or terrorism.

The full Act is available on the government's [Legislation](#) website.

Data Controller

The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data.¹²

Data Protection Impact Assessment

Formerly known as a Privacy Impact Assessment (PIA) a Data Protection Impact Assessment (DPIA) is a tool used when implementing data processing systems or information sharing process to risk assess them and ensure compliance with Data Protection legislation. They are mandatory for some types of processing and failure to conduct one correctly, or to consult the supervisory authority where required could all lead to fines from the Information Commissioner's Office.

¹² Adapted from GDPR Article 4(7).



Data Subject

An identifiable natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.¹³

Direct Care

Data Protection legislation allows processing when it 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.¹⁴ Within health and social care this can be understood as an activity concerned with the prevention, investigation and treatment of illness and the alleviation of suffering of individuals, including supporting individuals' ability to function and improve their participation in life and society.

It includes the assurance of safe and high quality care and treatment through local audit, the management of untoward or adverse incidents, person satisfaction including measurement of outcomes undertaken by one or more registered and regulated health or social care professionals and their team with whom the individual has a legitimate relationship for their care.¹⁵ As a concept, Direct Care is understood as being within a single organisation, although sharing is promoted for the continuation of care when service users are being transferred between organisations and / or where multiple organisations work together to provide the care.

¹³ Adapted from GDPR Article 4(1)

¹⁴ Adapted from GDPR Article 9(2)(h).

¹⁵ Adapted from Independent Information Governance Oversight Panel (2013), *Information: to Share or Not to Share* (Caldicott2 Report), p.128.



Encryption

A mathematical function using a secret value (the key) which encodes data so that only users with access to that key can read the information. In many cases encryption can provide an appropriate safeguard against the unauthorised or unlawful processing of Personal Data, especially in cases where it is not possible to implement alternative measures.¹⁶

Freedom of Information Act 2000

With some exemptions, the Act gives individuals, wherever they are in the world, rights of access to know whether information is held by public authorities, and copies of that information. The full Act is available on the government's [Legislation](#) website.

General Data Protection Regulation 2016

The General Data Protection Regulation is a regulation by which the European Parliament, the Council of the EU and the European Commission intend to strengthen and unify data protection for all individuals within the EU. It is the main piece of Data Protection legislation, replacing Data Protection Act 1998 as of 25 May 2018; this will be the basis for a new Data Protection Act. The main principles with regard to the processing of Personal Data are:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality

The Regulations introduces the concept of Accountability, which incorporates these principles, with which the organisation must demonstrate compliance. Alongside these, Data Subjects have eight specific rights to information, access, rectification, be forgotten, restriction of processing, notification, data portability, objection and to appropriate decision making. The full text is available in the [Official Journal of the European Union](#).

¹⁶ Adapted from 'Encryption' Information Commissioner's Office Website, accessed 11/07/2017 (see <https://ico.org.uk/for-organisations/guide-to-data-protection/encryption/>).



**Health and Social
Care Act 2012**

South East Coast Ambulance Service NHS
NHS For Health Trust

The Act provided for a wide-scale reorganisation of the NHS, abolishing Primary Care Trusts and Strategic Health Authorities, transferring their budgets to Clinical Commissioning Groups. With regard to Information Sharing the Act's main impact was to remove any legal basis for Clinical Commissioning Groups to receive patient-level information for commissioning purposes. The full Act is available on the government's [Legislation](#) website.

**Health and Social
Care (Safety and
Quality) Act 2015**

The Act places onto a legislative footing the requirement of the seventh Caldicott Principle, that the duty to share information can be as important as the duty to protect patient confidentiality. The full Act is available on the government's [Legislation](#) website.

**Human Rights
Act 1998**

The main provision of relevance is the individuals' Article 8 right to respect for their private and family life, home and correspondence. The full Act is available on the government's [Legislation](#) website.

**Information
Commissioner's
Office**

A non-departmental public body, which reports directly to parliament and sponsored by the Department for Digital, Culture, Media and Sport, that is the independent national data protection supervisory authority dealing with the new Data Protection Act, the Privacy and Electronic Communications Regulations 2003, the Freedom of Information Act 2000 and the Environmental Information Regulations 2004.

**Mental Capacity
Act 2005**

The Act impacts on all staff working with or caring for adults (16+) who have impaired capacity to make their own decisions about health, social care and financial matters, making it clear who has authority to make decisions for them. The full Act is available on the government's [Legislation](#) website.



Personal Data

Any information relating to a Data Subject who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.¹⁷

Personal Confidential Data

A collective term, building in line with the new Data Protection legislation on the concept within the Caldicott2 Report, encapsulating Personal Data and Special Categories of Data (herewith). It is broader than the new legislation's definitions of these as it incorporates an obligation of confidentiality around information concerning the deceased, about whom a similar duty is owed under Common Law.

Pseudonymisation

The process of distinguishing individuals in a dataset by using a unique identifier, which does not reveal their 'real world' identity.¹⁸

Privacy and Electronic Communication Regulations 2003

The Regulations compliment Data Protection legislation, giving people specific privacy rights in relation to electronic communications, with specific rules on:

- Marketing calls, emails, texts and faxes
- Cookies and the like
- Keeping communications services secure
- Customer privacy as regards traffic and location data, itemised billing, line identification, and directory listings.

The full Regulation is available on the government's [Legislation](#) website.

¹⁷ Adapted from GDPR Article 4(1).

¹⁸ Information Commissioner's Office (2012), *Anonymisation: Managing Data Protection Risk Code of Practice*, p.49.



Processing

Any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.¹⁹

Secondary Uses

Any use of Personal Confidential Data which does not directly contribute to the diagnosis, care and treatment of an individual and the audit / assurance of the quality of the healthcare provided to the individual.²⁰ It includes, but is not limited to:

- Planning and service development.
- Profiling, including tasks such as risk stratification and identifying frequent service users.
- Cross-organisational pathway planning.
- Cross-organisational system-wide service planning.
- Sharing of unique identifiers such as hospital or NHS numbers.
- Finance and invoicing.
- Cross-organisational outcomes / learning.
- Tasks that are logical and ethical, but for which it is not immediately apparent where the legal basis for completing them lies.

Special Categories of Data

Formerly known as Sensitive Data, this is Personal Data revealing a Data Subject's racial / ethnic origin, political opinion, religious / philosophical belief, trade union membership, genetics or biometrics (solely used to identify them), health, sex life and / or sexual orientation.²¹

¹⁹ Adapted from GDPR Article 4(2).

²⁰ Adapted from National Information Governance Board (2011). *Information governance for Transition*, p.42.

²¹ Adapted from GDPR Article 9(1).



Appendix 2: South East Coast Ambulance Service NHS Foundation Trust and [Organisation] Information Sharing Protocol Sign-Up Sheet

The completion and returning of this sign-up sheet indicates that the signatory's organisation accepts the terms and principles of South East Coast Ambulance Service NHS Foundation Trust IBIS Information Sharing Protocol (v1.0).

Sign-up should be from a member of staff at an appropriate level within the organisation, e.g. Chief Executive, Caldicott Guardian or Senior Information Risk Owner.

A schedule of signatories is maintained by the Information Governance Lead, South East Coast Ambulance Service NHS Foundation Trust.

- **Ambulance Trust:** South East Coast Ambulance NHS Foundation Trust (Information Governance Lead).
- **Mental Health Trusts**
- **Acute Trusts**
- **Community Trusts**
- **GP Practices**

It was subsequently:

- Agreed electronically as appropriately by partner organisations. IG Lead and SIRO



Appendix G: Patient Advice Leaflet



Patient Advice Leaflet

Patient Name:	
Name of Case Manager:	
Name of Care Team:	

Your Health Care Professional/Care Team has asked you about sharing information about your health needs with South East Coast Ambulance Service. Your agreement to do this will ensure that if you need to call 999 in future, the ambulance crew will have the right information to help make the best decision about your care needs.

You can be reassured that South East Coast Ambulance Service will:

- ✓ only access your information when you call 999
- ✓ only share this information with your GP or health professional, and only as a result of a 999 call
- ✓ retain your information in line with its health records policy
- ✓ store your information using secure methods
- ✓ allow you to view your information – please see the contact information below
- ✓ remove your information if you wish to withdraw your consent at any time.

If you have any queries about how we use your information or about South East Coast Ambulance Service in general, you can contact us via our Patient Experience Team:

Telephone: 0300 123 9242

Email: pet@secamb.nhs.uk

Or you can write to:

Patient Experience Team
Ambulance Headquarters
Nexus House
4 Gatwick Road
Crawley
RH10 9BG

There is also information on our website:

www.secamb.nhs.uk/contact_us/patient_advice.aspx