SCW

NHS
Hampshire and Isle of Wight
Partnership of Clinical Commissioning Groups

Information Asset Owner and Data Custodian Handbook

Version 4.3 – January 2020

Document type:	Guidance Document
Document title:	**Information Asset Owner and Data Custodian Handbook**
Document date:	09 May 2018
Author:	Information Governance team
Approved by:	**H&IoW Partnership of CCGs ISGS**
Approval date:	January 2020
Version:	**V4.3**
Next Review date:	August 2020

Version Control

Version	Date Issued	Brief Summary of Change	Author
V1.7	May 15	Update to key staff list on page 29 and IG structure chart	Cath Mitchinson
V1.8	June 15	Update to key staff list on page 29	Cath Mitchinson
V1.9	June 15	Update to key staff list on page 29	Cath Mitchinson
V1.10	August 15		Nicola Johnson
V1.2	November 2015		Nicola Johnson
V1.3	April 2016		Nicola Johnson
V2.0	August 2016	Contents re-ordered and re-formatted to create user friendly resource document	IG Team
V3.0	July 2017	Annual review, addition of 2017-18 DC Workplan, IG Structure and TNA	Matt Wall SCW IG Manager
V4.0	May 2018	Full review, updates and compression to ensure alignment with GDPR	Matt Wall SCW IG Manager
V4.1	July 2019	Annual review incorporating changes following SCW review (Data Processing agreements)	Matt Wall SCW IG Manager
V4.2	Sept 2019	Update to page 4 introduction, removed IG structures and DC/IAO list, link provided to Partnership IG Intranet page for further information	Matt Wall SCW IG Manager
V4.3	Dec 2019	Removal of references to North East Hants & Farnham CCG, updates to DPO and SIRO details	Hayley Matthews SCW IG Manager

Contents

Section 1: Introduction 4

Section 2: IG Roles and Responsibilities: 6

Section 3: DC Work Programme 11

Section 4: DC Ongoing Processes 16

Appendix A – IG Key Contacts List 23

Appendix B – Annual Task List 2018/19 24

Appendix C – Data Security Protection Toolkit Assertions 25

Appendix D – Training Needs Analysis 2018/19 28

Acknowledgement receipt 29

Section 1: Introduction

This handbook applies to all Clinical Commissioning Groups, hereafter 'the CCG', who are part of the Hampshire and Isle of Wight Partnership of CCGs, hereafter 'the partnership' The Hampshire and Isle of Wight Partnership of CCGs is comprised of North Hampshire CCG; Fareham & Gosport CCG; South Eastern Hampshire CCG and Isle of Wight CCG. All CCGs in the Partnership will adhere to the individual legal and statutory obligations of their respective organisations.

This Staff handbook contains the advice and guidance to support the roles and responsibilities of the Information Asset Owners (IAOs) and Data Custodians (DCs) within the Partnership CCGs and explains how the IAO's and DC's support the Information Governance work plan, framework and the organisations' Data Security & Protection (DSP) Toolkit submission

This handbook should be read in conjunction with the Information Governance (IG) Staff handbook which describes the IG practice used by all organisations to ensure that information is efficiently managed and appropriate policies, system processes and effective management accountability provide a robust governance framework for safeguarding information.

Additional information, advice and guidance can be sought from the Partnerships Data Protection Officer (DPO) in the first instance or where required, the SCW Information Governance (IG) Manager.

This pack contains specific sections which outline the roles and responsibilities within the CCG and associated activities. The following appendices contain;

Appendix A – key IG staff
Appendix B – Annual task list
Appendix C – Data Security Protection Toolkit Assertions
Appendix D – Training Needs Analysis

For individual CCG Information Governance Structures and further information, guidance and policies please visit the Information Governance page on the H&IoW Partnership Intranet at http://intranet.hiowccgpartnership.nhs.uk/information/governance/information-governance or contact your CCGs IG Manager.

Information and its Purpose within the Organisation

Every staff member uses various forms of information in order to carry out their work functions on a daily basis. Information is fundamental to the successful operation of the organisation without which, it would not be able to support the health needs of the local population.

The developments within Information Technology have enabled organisations to work more collaboratively with partners, communicate and share information more effectively, provide and analyse more accurate data information, and has also enhanced the organisation's performance and productivity.

The CCGs holds personal data and special categories of persona data. It is, therefore, vital the CCGs in the Partnership can ensure that data protection practices are adequate and this information is handled in the correct and most appropriate way. It is important for the workforce to be made aware of what constitutes personal data, special categories of data and commercially confidential data. Please refer to the IG Staff handbook for specific guidance on these terminologies.

Adherence to IG principles ensures compliance with legislation, best practice and embeds processes that help staff manage personal data, special categories of data and commercially confidential data appropriately, thus enabling patients and service users to have greater trust in the organisation in relation to their information. This appropriate use should also include effective collaborative working across the CCGs and partner organisations, improving information sharing, quality and accuracy of data.

Data Security and Protection (DSP) Toolkit

The Data Security and Protection Toolkit is an online self-assessment tool that allows organisations to measure their performance against the National Data Guardian's 10 data security standards.

All organisations that have access to NHS patient data and systems must use this toolkit to provide assurance that they are practising good data security and that personal information is handled correctly.

All organisations are required to complete a final submission by March of the reporting year with the final responses and approval for the submission being agreed by the CCG's SIRO.

The IAOs and DC/IAAs support the individual CCGs toolkit submission in undertaking activities and collecting evidence within their teams. The annual task list is shown in Appendix B.

In the 10 standards, there are 43 assertions and 106 mandatory sub-requirements for the CCGs to complete requiring different types of evidence; including but not limited to statements of compliance, minutes, electronic communication, information asset register, data flow mapping documentation, data sharing agreements etc. A complete listing of the current assertions is included at Appendix C.

IG Staff Handbook: Training & Awareness

IG Staff Handbook

This is given to all new staff on their commencement of employment within each CCG. It is a comprehensive introduction to Information Governance as it contains the relevant information to allow staff to perform their duties within the law. It contains details of:

- Guide to the Legislation and Regulations
- The Caldicott Guardian and Data Protection Legislation principles
- Guide to Confidentiality
- Individuals rights under GDPR
- Information Sharing and Data Sharing Agreements
- IT Security
- Business Continuity Plans
- Breaches of Security or Confidentiality

It is updated on an annual basis to ensure that it reflects current requirements. Additional versions may be issued before that time, if and when changes in legislation or national guidance occur. Staff will be notified that a new version is available on the intranet and via email, each IAO/DC should ensure their teams are aware and should review the revised handbook.

Mandatory Information Governance Training

Every individual who works for the CCGs in the Partnership is required to complete the mandatory (IG) training annually (entitled Data Security Awareness level 1). This includes new starters, existing and temporary members of staff, lay members and all contractors.

The Partnership CCGs have a responsibility for ensuring that those working with its information are aware of the Data Protection Legislation principles and the risks or incidents which may occur if IG processes are not followed.

All new starters are expected to complete the four data security awareness training modules via the ConsultOD or e-LfH portal within their first 2 weeks of employment. Annual mandatory training for all staff is provided through the ConsultOD or e-LfH portal, which include individual comprehension/assessment tests.

We have conducted a training needs analysis (TNA) and identified IG training that needs to be completed by staff in different job roles and functions – this includes specific modules/workbooks for staff accessing or using special categories of personal data. The TNA can be found at Appendix D.

DCs/IAAs are responsible for monitoring compliance with IG training within their teams and should encourage staff to complete mandatory training as soon as possible, but definitely by the end of the 1st quarter in each financial year.

Section 2: IG Roles and Responsibilities:

Summary of Information Governance Roles

Role	Summary
Accountable Officer	Has overall responsibility for Information Governance within the organisation. As Accountable Officer, they are responsible for the management of the organisation and for ensuring appropriate mechanisms are in place to support service delivery and continuity. The management of information risk and information governance practice is now required within the Statement of Internal Control which the Accountable Officer is required to sign annually.
The Managing Director	Has lead responsibility for the CCG they manage and will work closely with the Clinical Chair/s ensuring that the services delivered provide the most effective use of resources to meet local needs.
Information Risk Owner (SIRO)	The Senior Information Risk Owner for the Partnership is an executive board member with allocated lead responsibility for the organisation's information risks and provides the focus for management of information risk at Board level. The SIRO must provide the Accountable Officer with assurance that information risk is being managed appropriately and effectively across the organisation and for any services contracted by the organisation. The SIRO is corporately responsible for the Information Asset Register and the Dataflow Map and are supported by IAOs

Caldicott Guardian	The Caldicott Guardians are the persons within the Partnership with overall responsibility for protecting the confidentiality of personal data and special categories of personal data (described as Personal Confidential Data (PCD)) in the Caldicott 2 report, and for ensuring it is shared appropriately and in a secure manner. This role has the responsibility to advise the Partnership Board and relevant committees on confidentiality issues. The SCW Information Governance Manager will support the Caldicott Guardian in fulfilling this role.
Data Protection Officer	The Data Protection Officer (DPO) is the person that has been assigned the responsibilities set out in the GDPR, such as monitoring and assuring compliance with IG legislation, providing advice and recommendations on Data Protection Impact Assessments, giving due regard to the risks associated with the processing of data undertaken by the organisation and acting as the contact point with the and ICO.
SCW Information Governance Manager	The SCW Information Governance (IG) Managers support the Partnership DPO in ensuring that the Information Governance programme is implemented throughout the Partnership and Individual CCG's therein. The IG Managers also co-ordinate a number of activities that contribute to the completion and annual submission of the Data Security and Protection Toolkit for the individual CCGs. The IG Managers will support the Partnership SIRO, Caldicott Guardians and DPO in investigating Serious Incidents Requiring Investigation (SIRIs), offer advice and ensure the organisation complies with legislation, policies and protocols as per the SLA.
Cyber Security Manager	Act as a central point of contact on IT security within the organisation and for external organisations that has entered into an agreement for the provision of IT services by the SCW CSU. They will implement an effective framework for the management of security. They assist in the formulation of Information Security Policy and related policies. They will advise on the content and implementation of the Information Security Programme and co-ordinate IT security activities particularly those related to shared information systems or IT infrastructures. They liaise with external organisations on IT security matters, including representing the organisation on cross-community committees. Provide advice to users of information systems, applications and Networks of their responsibilities, create, maintain, give guidance on and oversee the implementation of IT Security and ensure that risks to IT systems are reduced to an acceptable level by applying security countermeasures identified following an assessment of the risk. They will also ensure breaches of policy and recommended actions are reported in line with organisation's procedures.
Information Asset Owners (IAO)	The SIRO is supported by Information Asset Owners (IAOs). The role of the IAO is to understand what information is held, what is added and what is removed, who has access and why in their own area. As a result they are able to understand and address risks to the information assets they 'own' and to provide assurance to the SIRO on the security and use of the assets. See below for details of IOA responsibilities

Data Custodians (DC's)	This important role is required to support the IAO's and SIRO to fulfil IG responsibilities and to ensure staff apply the Data Protection Legislation and Caldicott Principles within working practices. See below for details of DC / IAA responsibilities.

Information Asset Owners (IAOs)

IAOs have the responsibility to provide assurance that information risk and the handling of information requirements are managed effectively. Each team/system will have a designated IAO.

Aspect of IAO role	Responsibilities
Who are Information Asset Owners?	The IAO is a senior member of staff who is the nominated owner within their team for one or more identified information assets of the organisation.
What are IAOs responsible for?	The IAO is expected to understand the overall business goals of the organisation and how the information assets they own contribute to and affect these goals.
	To foster an effective IG culture for staff and others who access or use their Information Assets to ensure individual responsibilities are understood, and that good working practices are adopted in accordance with the organisation's policy.
	Ensure that staff and relevant others are aware of and comply with expected IG working practices for the effective use of owned Information Assets. This includes records of the information disclosed from an asset where this is permitted
	The IAO must be aware of IG related legislation and regulations that stipulate how organisations: • should safeguard information, • the processes that are in place to use, secure and transfer information, • how patients and members of public can access personal/business information
	Ensure compliance with their CCG's Information and Cyber Security Policy and thereby maintain controls by ensuring risks identified are included are included on the appropriate risk registers to provide: • Optimum confidentiality of information • Review information sharing procedures • Optimum system integrity • Optimum availability of information • Appropriate use of equipment by appropriately trained personnel • System security reviews • Develop and maintain system specific risk assessments

Incident Management	Ensure that the organisation's requirements for information incident identification, reporting, management and response apply to the Information Assets they own. This includes the mechanisms to identify and minimise the severity of an incident and the points at which assistance or escalation may be required.
What are the roles and tasks of an IAO	Manage the core IG objective that all information assets are identified and that the business importance of those assets is established. Ensure there is comprehensive asset ownership and clear understanding of responsibilities and accountabilities. (This is especially important where information assets are shared by multiple parts of the organisation).
	Provide a focal point for the resolution and/or discussion of risk issues affecting their Information Assets
	Take ownership of their local asset control, risk assessment and management processes for the Information Assets they own. This includes the identification, review and prioritisation of perceived risks and oversight of actions agreed to mitigate those risks
	Identify and document the scope and importance of all Information Assets they own in an Information Asset Register, including identifying how to respond to incidents or recover from a disaster affecting the Information Asset.
	Support the SIRO in their overall information risk management function, together with other relevant people both internal and external.
	Support DCs in the completion and maintenance of the Information Asset Register and Dataflow Maps and with any DPIAs that the department may require
	Ensure that all their entries on the Information Asset Register and Data flow Map are correct, updating where necessary and consulting the DPO where a new information asset is likely to emerge
What training does an IAO need to complete?	In addition to the mandatory annual training IAO's are required to undertake the 'Introduction to Risk Management for SIROs and IAOs - Workbook' NHS Digital Workbook every three years to demonstrate their skills and capabilities are up to date, and relevant to the needs of the information assets they own.

<u>Data Custodians (DCs)</u>

Aspect of DC role	Responsibilities
Who are they?	• They are local IG champions who have been nominated by their IAO, to support the Implementation of the IG agenda within their Teams. • They are accountable to the Senior Information Risk Owner (SIRO) via their

	IAO.
What are they responsible for?	• Embedding the IG work programme within their teams. • Providing assurance to their IAO and the SIRO that information risk is managed effectively • Auditing staff compliance with information handling standards. • Ensuring that colleagues complete mandatory and recommended IG training modules/workbooks by December. • Providing an IG update at team meetings to discuss areas of concern within their respective areas of work, whilst exchanging methods and good practice. • Serving as local records managers ensuring the accurate storage and retention of records and their content • to provide assurance that information risk and the handling of information requirements are managed effectively • Directly support the implementation of IG within their CCG and team.
Role and Responsibilities	Ensure that all the staff within your work area: • know the name and contact number of their IAO, DPO, Caldicott Guardian, SIRO and SCW IG Manager • are aware that IAO's are the first point of contact for any queries regarding IG • apply and embed the Data Protection Legislation and Caldicott Principles within their working practices • abide by the relevant policies that contribute to the effective implementation of IG • attend training where appropriate • inform them of starters and leavers, then to provide the IG Team with this information • complete the annual 'Data Security Awareness level 1 modules and other applicable modules as shown on the TNA (Appendix D) Positively promote IG by ensuring that: • Information is regularly cascaded at team meetings • promotional materials provided are utilised to inform staff within the team • Regularly meet and support their IAO as required • Process Requests made under the data subjects Rights as set out in the GDPR and in line with the procedure and ensure staff are aware of their responsibilities to support subject access requests • Play an active role in the development of IG campaigns across the organisation • Keep up to date with policy development and where possible contribute to the process to ensure that any gap between policy and practice is closed • Participate in the collating of evidence for the DSP Toolkit for the team - this will be supported by SCW IG Team • Staff seek permission from their IAO or DC to transfer personal and sensitive information held on a portable device
What does the	Key tasks are to:

Work Programme comprise of?	a) Complete and Maintain: I. Information Asset Register II. Data Flow Mapping III. Training Awareness Record b) Complete: I. Confidentiality and Safe Haven Audit II. IG Spot Check and Record Keeping Audit c) Monitor staff IG training compliance d) Assist with: I. Incident Management II. Requests made data subjects Rights as set out in the GDPR III. Data Protection Impact Assessments IV. System Level Security Policies V. Business Continuity Management
How much time will the role take?	This will vary. Time will need to be taken to inform/discuss information governance updates and changes to legislation, and some additional time spent arranging training and completing tasks. The main responsibility is to conduct audits within their assigned areas, for example, auditing information assets and information governance working practices.
Where can I find the necessary templates and documentation?	The necessary policies, procedures, templates and other documentation are available on the IG page on the CCG/Partnership Internet and in all staff digital folders
Who do I report an IG breach or an identified information risk?	You should immediately contact the Information Governance team, who will log the incident and escalate it to the Data Protection Officer. They should also follow (and encourage others to follow) the Partnerships Incident Management process.
What training does a DC/IAA need to complete?	In addition to the mandatory annual training, DC's are required to attend the DC induction presentation once and complete the DC questionnaire every three years to demonstrate their skills and capabilities are up to date, and relevant to the needs of the information assets they own.

Section 3: DC Work Programme

Information Assets and Information Asset Register (IAR)

Subject Heading	Definition and Actions needed to complete the audit process
What is an Information Asset Register (IAR) and why is it completed?	Keeping an IAR enables the Individual CCGs to understand what information and assets are held and how it supports operations within your team.
	It supports 'data mapping, as well as help prevent loss of information and IG breaches. It will also help to fulfil Freedom of Information act requests in a

	timely manner. All information assets will be 'owned' by your team's IAO.
Why is an audit of the assets undertaken?	DC/IAAs are required to identify and record information assets within the information asset register template provided. This practice is used to: • ensure that the information assets within the CCG are managed effectively, • identify potential issues, • protect and keep assets secure.
What happens to the information contained in it?	Once the audit of equipment and information has been completed, the information asset register will need to be maintained and will be used as evidence as part of the DSP toolkit submission.
How do I complete the IAR?	The first step is to identify what the information assets are within your team, these would include anything that is an ''asset'' to the organisation, such as: • A corporate record • A database of contact details (this can be considered as a single information asset) • Documentation/information associated with a specific project (such as spreadsheets, graphs, emails etc.) can also be considered a single asset • Computers, Laptops, USB etc. will need to be recorded (as do their asset numbers)
How do I assess if it is an asset?	When assessing an asset it is key to consider the following questions • Would the organisation consider the information to be 'valuable'? • What is the information for? • What effect on operations would it have within your team if the asset did not exist or if it was not easily accessible? • Is it possible to identify any associated risks in using the information asset?
	It is important to note that pieces of information may be grouped to form a single information asset. By incorporating individual information to form an information asset it is easier to manage, audit and identify potential issues which may require further assessment by the IG team or through the CCG Risk Management process.
	However, it is also important to note that some information will need to be split further down as it would be a larger risk to consider (i.e. a whole filing management system, as a single information asset is too large (e.g. the shared drive).
	Information assets should be grouped and considered according to operational need not technological elements i.e. used by computer etc. DCs must also consider that individual information could be included within two different information assets. In order for effective management, it would be useful to include the individual information in one asset and reference it to the other information asset.

Data Flow Mapping Exercise (DFM)

Subject Heading	Definition and Actions needed to complete the audit process
Why do we complete the Data Flow mapping process?	It is a requirement under the Data Protection Legislation for organisations to be accountable and where they are Processors, be able to provide accurate and up to date data processing records. All organisations must implement data-protection principles and embed measures to avoid unauthorised and unlawful: • access • transfer • processing of • accidental loss and destruction of • damage to personal data
How does the DFM exercise produce the outcomes to inform CCG of the risks?	All questions on the template will need to be answered for each data flow, spreadsheet will automatically RAG rate each data flow using the CCG’s 5*5 risk matrix.
	Once completed any data flows that score a Moderate Risk (yellow) to Extreme Risk (Red) must be mitigated by the IAO, discussed with DPO supported by the IG Manager and escalated through the Partnerships risk management process as appropriate.
What information is included in this process?	Data Flow Maps record all inbound and outbound flows of data throughout the individual CCGs and will include; • The where, why, how and with whom the organisation exchanges information. • A risk assessment on all data flows and • The legal basis for the data to flow

Staff IG Awareness Spot Checks

The CCG has a legal obligation to ensure that it manages and safeguards confidential data and has procedures in place to highlight problems such as incidents, complaints or breaches.

Subject Heading	Definition and Actions needed to complete the audit process
Safe Haven	It is the individual CCGs responsibility to ensure that its information is safe and is transferred in a secure way. Various methods are used to share confidential personal data, special categories of personal data and commercially confidential information and it is important to ensure that we follow the Safe Haven Policy and procedures.
	The Information Commissioners Office (ICO) has reported a number of insecure transfers of information via fax, post and emails and has imposed monetary penalties on organisations who have failed to comply with the Data Protection Legislation.
What does Safe Haven mean?	A ‘Safe Haven’ is a term used to explain either a secure physical location or the agreed set of administration arrangements that are in place within the organisation to ensure information is communicated/transferred safely and securely.

	It is a safeguard for information, which enters or leaves the organisation whether this is by telephone, fax, post, email, spoken communication and other means.
Complying with the Safe Haven requirements	There are two documents available on the CCG/Partnership internet to ensure compliance with the requirements: • Confidentiality & Safe Haven Policy • IG Staff Handbook
Conducting IG awareness audit	Ensuring your staff are aware of safe haven processes is important to establish whether suitable protocols, procedures and induction processes are currently in place and that they are being adhered to by staff. The audit is easy to follow and consists of specific questions that need to be completed to ensure the CCG maintains compliance with confidentiality and safe haven requirements
	The completed audit should be signed off by the IAO before submitting it to the local SCW IG Manager
Requirements within the Safe Haven policy:	The Confidentiality and Safe Haven Audit template has been designed to incorporate all the requirements as set out within the Safe Haven policy. The processes that will need to be addressed when discussing working practices with staff are: • Safe Haven Fax Process • Safe Haven Post Process • Safe Haven Computer Process • NHS mail Process For further information and guidance refer to the Confidentiality & Safe Haven policy located on the CCG/Partnership internet or contact the DPO supported by the SCW IG Manager
What is my role regarding staff awareness?	You should ensure that all staff are trained and made aware of confidentiality and safe haven requirements and procedures.

IG Spot-check and Record Keeping Audit

Subject Heading	**Definition and Actions needed to complete the audit process**
Who should carry out the audit?	Each DC/IAA will undertake an audit of these processes within their assigned team
What is the purpose of this audit?	The Audit supports the DSP toolkit submission and helps to; • Identify and monitor colleagues and their compliance with IG protocols • Understand what records are available within your assigned area • Assess the staff knowledge of records management • Identify if the Partnerships Records Management Policy and procedures are adhered to by staff and have been implemented within your assigned area • Identify any gaps in the record management processes

	• Captures the responses from the staff awareness questions
What happens to the audit when it is completed?	The completed audit should be signed off by the IAO before submitting it to the local SCW IG Manager.

Business Continuity Plans (BCP's)

Subject Heading	Definition and Actions needed to complete the process
What is business continuity?	It is a method used to identify potential impacts that may threaten the operations of, or the organisation itself. The fundamental element of business continuity is to ensure that whatever impacts upon the organisation, the business continues to operate. Business continuity plans will help shape organisational resilience to 'threats' and plan counteractions to minimise interruptions to an organisation's business activities from the effects of major failures or disruption to its Information Assets (e.g. data, data processing facilities and communications). Business Continuity Plans are frameworks for your business function within the organisation and incorporates every element.
Why does the CCG need to complete BCP?	Departmental BCP's form part of the DSP Toolkit assertions and support the organisational BCP as appendixes.
What role does the DC/IAA have in the BCP?	Although it is not the role of DCs to produce a BCP for your team, they are asked support the IAO in ensuring that the IG elements are considered and incorporated within the departmental BCP. This will coincide with some of the exercises and audits being carried out.
How will my role encompass the BCP aspect?	As part of the DSP Toolkit assertion, DCs are asked to collate the following: • A list of critical information assets (this includes information assets which are critical to the functionality of your assigned area). Identify and document all the critical resources you need to run your business. This may include computer systems and files, physical documents, specialist equipment etc., i.e. the things that would severely disrupt your work if you no longer had them and could not easily replace them. These resources are also likely to include your key staff - what would you do if several staff were absent due to sickness at the same time? If access to resources was restricted temporarily, how long could you manage without them before you needed to take some emergency action? • Advise and support the IAO's to analyse the effect that a disruption might have upon their business function and complete the departmental BCP • Ensure that staff are aware of and can locate the departmental and organisational BCP
ow do I get access to the BCP	The departmental BCP template has been designed to incorporate the elements stated above and is available via the resilience/Governance Lead for the CCG/Partnership.

template?	

Section 4: DC Ongoing Processes

Reporting IG Incidents & Breaches

Subject Heading	Definition and Actions needed to complete the process
Who should be notified of any IG incidents or breaches?	The CCG's IG Manager at the earliest opportunity who will escalate to the CCG's SIRO, Caldicott Guardian & DPO as appropriate
What type of incident should be reported?	Incidents that relate to IG, Cyber Security and Data Protection Legislation breaches.
How do I get further information?	For further guidance on reporting IG incidents please refer to the Partnerships procedure for reporting information incidents, which reflects the NHS Digital checklist guidance for reporting, managing and investigating information governance and cyber security serious incident requiring investigations (SIRI) The Partnerships Information Incident Management and Reporting Procedures are available on the CCG/Partnership intranet
How do I encourage colleagues to report incidents?	Provide them with sufficient information to understand how reporting incidents will improve working practices and reduce complaints.
Who will be responsible for logging incidents with NHS Digital	The SCW IG Manager will log any Level 2 IG incidents on the national SIRI system after discussion with the Partnerships DPO, SIRO and Caldicott Guardian(s).

Individual Rights including Subject Access Requests

Subject Area	Explanation
What is a Data Subject Access Request?	Any enquiry made by a patient or member of staff with regard to access to their personal data, will be considered as a Data Subject Access Request. The Data Protection Legislation provides rights of access by the data subject to their personal data and to be provided with copies of their information.
What is the required format for a DSAR?	All requests for information must be made in writing and any written enquiry that asks for information you hold about the person will be construed as a Data Subject Access Request.

What do I do when I receive a Subject Access Request?	You should ensure that you read and follow the Data Subject Access Request Policy which can be found on the CCG/Partnership intranet. This sets out the process for handling SARs, including flow charts on how and who to send requests too and template letters for your use.
What are the key processes?	• Log the request • Seek proof of identification (and authority to act where required) • Request the information from the appropriate service or team • Review the information for third party information and other information that may require redaction • Explain any complex terms or codes • Respond within **one** calendar month • Transfer the information securely
Do requests have to be responded to within certain timescales?	Under the Data Protection Legislation DSAR's must be complied with within one calendar month. By not adhering to this deadlines, the organisation will have failed to comply with the Data Protection Legislation and may be subject to complaints to and possible investigation by the Information Commissioner's Office (ICO)
What records do I need to keep?	A log of all Data Subject Access Requests handled for your team. The SCW IG team will request quarterly DSAR figures for reporting into the ISGS
Where do I get further advice & guidance?	Contact a member of the CCGs Governance Team, SCW IG Manager or SCW IG Team if you are in any doubt.

Records Management

Subject Heading	Definition and Actions needed to complete the process
What is Records Management?	This is the process by which an organisation manages all the aspects of records whether internally or externally generated and in any format or media type, from their creation, all the way through to their lifecycle to their eventual disposal. It is the aims of the organisation to ensure that records are accurate and reliable, can be retrieved swiftly and kept for no longer than necessary
What are the consequences if records are not properly maintained?	Records Management is crucial to all NHS organisations. If records are not managed effectively the Partnership would not be able to function as required or expected. Records are required to provide evidence of actions and decisions, enable the Individual CCGs to be accountable and transparent, and comply with legal and regulatory obligations such as the Data Protection Act Legislation and the Freedom of Information Act 2000.
What form are records	Records within the NHS can be held in paper or electronic form and as the

held in?	National Care Record Guarantee has been implemented; all NHS organisations have a duty to ensure that their record systems, policies and procedures comply with the requirements identified within it.
What are the two categories of records held within NHS?	1. Corporate Records can be considered records which contain the following: • all administrative records (e.g. personnel, estates, financial and accounting records, notes associated with complaints) 2. Health records can be considered records which contain the following: • All patient health records (for all specialties and including private patients, including x-ray and imaging reports, registers, etc.)
How will this area of work help me with my role?	Good Records Management will also help with the Information Asset Audit and the Data Flow Mapping exercise.
Where will I find further details of the Records Management process?	The Staff IG handbook contains further information together with the Partnerships Records management Policy which is informed by the NHS Records Management Code of Practice which can be found here.
What type of documentation exists for tracking paper records?	A record tracker template for monitoring paper records can be provided by the IG team

Data Sharing Agreements (DSA's)

Subject Heading	Definition and Actions needed to complete the process
What are DSA's?	A Data Sharing Agreement (DSA) is necessary where two or more Controllers wish to share data for a joint or individual purpose. They complement the contractual documents that must be put in place and are used to identify the roles and responsibilities each party has to the data being shared as well as the purposes for the sharing.
Why does the organisation need to use them?	The individual CCGs use DSA's to put in place an agreement between parties to document: • The purpose for sharing the information • Who the information will be shared with • Structures for sharing information • Legislation and regulations which must be adhered to • Caldicott Guardian or SIRO endorsement of the data sharing arrangements and acceptance of the organisations obligations

How will this area of work help me with my role?	This can be a complex and technical area and mistakes are common with regard to which organisation/s holds responsibilities for the data being shared. It is important to understand in your role what information is shared with/from partners of the CCG and this will intern support the completion of the IAR and the DFM exercise, you should check that DSA's are in place for relevant data flows. You may also carry out assessments on the information flows between the organisation and its partners and as a result support the completion of a local DSA.
What is the process for DSA approval?	You should be supported by the SCW IG Manager in preparing any agreement where it is proposed that the CCG is a data sharing partner. Final approval is then sought from the relevant Partnership Caldicott Guardian or SIRO after consultation with the DPO.
Where can I obtain the templates?	Templates and guidance are available from the SCW IG team. Please contact your CCGs IG Manager if you have any questions

Data Protection Impact Assessments (DPIA's)

Subject Heading	Definition and Actions needed to complete the process
What is a DPIA	A DPIA is a document that identifies the IG elements of a project/process. A template, guidance documents and other checklists to help with a DPIA are available from the CCG/Partnership intranet. The IAO and DPO can review and risk-assess DPIAs to help establish Information Governance implications at the start of a programme and project before they are approved
Why is a DPIA required?	Under the Data Protection Legislation the completion of a DPIA is a statutory requirement where the type of processing is likely to result in a high risk to the rights and freedoms of natural persons and in particular in the cases of: • Systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing • Processing on a large scale of special categories of data referred to in GDPR article 9(1), or article 10; or • Systematic monitoring of a publicly accessible area on a large scale.
What are the benefits of identifying and introducing a DPIA	Identifying information governance elements at an early stage will ensure; • Compliant operations • Necessary information sharing protocols and data processing agreements are in place • The CCG is aware of and can effectively monitor the use of information and data
	It will also reduce the potential for failing to comply with the Data Protection Legislation and subsequent investigation from the Information Commissioner's Office. NOTE: under section 157 of the Data Protection Act 2018, the ICO is able to impose a penalty for failing to complete a DPIA when it is mandated to do so under Article 35 of the GDPR. The maximum amount that can be imposed is 10 million Euro's or 2% of total annual worldwide turnover in the case of an undertaking or group of

	undertakings.
What is the process for DPIA approval?	Once the DPIA has been completed, the document must be forwarded to the Partnerships DPO for review. Some DPIAs might be submitted to the PIA panel for further assessment. Final approval must then be sought from the relevant Partnership Caldicott Guardian or SIRO

Data Processing Agreements (DPA's)

Subject Heading	Definition and Actions needed to complete the process
What are DPA's?	A Data Processing Agreement (DPA) is necessary where a Controller wishes to engage another organisation to process data on their behalf. The best example of this is the data that SCW Processes for the Partnership CCGs under contract. DPA's must be put in place to complement the contractual documents and are used to identify the roles and responsibilities each party has to the data being processed as well as the purposes for the processing.
Why does the organisation need to use them?	DPA's are an agreement between parties to: • Describe the purpose for processing the information • Give detailed instructions governing the processing • Ensure that Controller obligations are observed and • Identify the legislation and regulations which must be adhered to • Provide Caldicott Guardian or SIRO endorsement of the data processing arrangements and acceptance of the organisations obligations as Processors
How will this area of work help me with my role?	This can be a complex and technical area. It is however important to understand that if a processor is processing data on behalf of the CCG then it needs to have a formal contract in place in order to do this. Often there is a formal contract and a Data Processing Agreement that supports this. The detailed information is included in a Data Processing Schedule. It is entirely possible for one Data Processing Agreement to be put in place between the CCG and a processor with an infinite number of schedules depending on the services being delivered. Examples of this will be for contract and performance monitoring, for Individual Funding Requests, for HR and so on.
What is the process for DPA approval?	You should be supported by your CCG's IG Manager in preparing any agreement. Final approval is then sought from the relevant Partnership Caldicott Guardian or SIRO after consultation with the DPO.
Where can I obtain the templates?	Templates and guidance are available from the SCW IG team. Please contact the SCW IG Manager if you have any questions

Section 5: Glossary's & Appendices

Glossary of abbreviations

Abbreviation	Meaning
IAA	Information Asset Administrator (interchangeable term for Data Custodian)
BCM	Business Continuity Management
BCP	Business Continuity Plan
CCG	Clinical Commissioning Group
CSU	Commissioning Support Unit
DC	Data Custodian
DPA	Data Processing Agreement
DPA 2018	Data Protection Act 2018
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
DSA	Data Sharing Agreement
e-LfH	E learning for health (online training provider)
FOI/FOIA	Freedom of Information Act 2000
FPN	Fair Processing Notification (privacy notice)
GDPR	General Data Protection Regulations
GP	General Practitioner
IAO	Information Asset Owner
ICO	Information Commissioners Office
IG	Information Governance
IT	Information Technology
SCW	South, Central and West
SIRO	Senior Information Risk Owner

Glossary of Terms

Term	Meaning
Commercially confidential Information	Business/Commercial information, including that subject to statutory or regulatory obligations, which may be damaging to SCW CSU or a commercial partner if improperly accessed or shared. Also as defined in the Freedom of Information Act 2000 and the Environmental Information Regulations.
Controller	A controller determines the purposes and means of processing personal data. Previously known as Data Controller but re-defined under the GDPR.
Personal Confidential Data	Personal and Special Categories of Personal Data owed a duty of confidentiality (under the common law). This term describes personal information about identified or identifiable individuals, which should be kept private or secret. The definition includes dead as well as living people and 'confidential' includes information 'given in confidence' and 'that which is owed a duty of confidence'. The term is used in the Caldicott 2 Review: Information: to share or not to share (published March 2013).
Personal Data	Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural 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 natural person
Processor	A processor is responsible for processing personal data on behalf of a controller. Previously known as Data Processor but re-defined under the GDPR.
'Special Categories' of Personal Data	'Special Categories' of Personal Data is different from Personal Data and consists of information relating to: (a) The racial or ethnic origin of the data subject (b) Their political opinions (c) Their religious beliefs or other beliefs of a similar nature (d) Whether a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1998 (e) Genetic data (f) Biometric data for the purpose of uniquely identifying a natural person (g) Their physical or mental health or condition (h) Their sexual life

Appendix A – IG Key Contacts List

Name	Position	Base	Contact details
Roshan Patel	Senior Information Risk Owner	Hampsire County Council, The Castle, Winchester, SO23 8UJ	01252 335154 E:SIRO.HIOWPartnership@nhs.net
Julia Barton	Caldicott Guardian (All CCGs except IoW)	Commcen Building Fort Southwick James Callaghan Drive Fareham PO17 6AR	02392 282067 E:julia.barton1@nhs.net
Louise Spencer	Caldicott Guardian (IoW CCG)	The Apex, St Cross Business Park, Monks Brook, Newport, Isle of Wight, PO30 5XW	07786 398182 E: Louise.spencer2@nhs.net
Jackie Thomas	Data Protection Officer	Omega House, 112 Southampton Road, Eastleigh, Hampshire, SO50 5PB	07775 404825 E: Scwcsu.igenquiries@nhs.net
Greg Snelgrove	Head of Governance	Omega House, 112 Southampton Road, Eastleigh, Hampshire, SO50 5PB	Please contact IG Team (details below)
Lucy Long	IG Manager (SCW)	The Apex, St Cross Business Park, Monks Brook, Newport, Isle of Wight, PO30 5XW	M: 07768 173 387 E: **Lucy.Long@nhs.net**
Hayley Matthews	IG Manager (SCW)	Omega House, 112 Southampton Road, Eastleigh, Hampshire, SO50 5PB	M: 07796335625 **E:hayleymatthews@nhs.net**
Rachel Lloyd	IG Manager (SCW)	CommCen Building, Fort Southwick, James Callaghan Drive, Fareham, PO17 6AR	M: 07826953558 **E: Rachel.Lloyd@nhs.net**
SCW CSU IG Team		Omega House, 112 Southampton Road, Eastleigh, Hampshire, SO50 5PB	023 8062 7579 **Scwcsu.igenquiries@nhs.net**

Appendix B –Annual Task List 2019/20

Task	Start Date	Finish Date	Action
Information Asset Register & Information Asset Risk Assessment	May 2019	July/Aug 2019	1. Data Custodians to review the team Information Asset Register 2. IAOs to risk assess business critical assets highlighted by the review 3. IAOs to accept or mitigate risks highlighted by the review 4. IAOs sign off final version using approval template
Information Flow Mapping Exercise & Information Flow Risk Assessment	May 2019	July/Aug 2019	1. Data Custodians to review the team Data Flow Mapping 2. IAOs to accept or mitigate risks highlighted by the review 3. IAOs sign off final version using approval template
Annual IG Training	01/04/2019	31/07/2019	Data Custodians to ensure all staff complete mandatory training before 31/07/2019. Key staff modules for new IAOs & Data Custodians (once complete key modules are valid for 3 years). New Starters should be completed within 2 weeks of joining
IG Staff Handbook Receipts	Ongoing for new starters		Data Custodians to ensure all new starters complete the staff IG handbook receipt and return to IG Lead
IG Spot Check Audit	July/Aug 2019	Nov 2019	1. Data Custodians to conduct IG Spot Check & Record Keeping Audit 2. IAOs sign off final version using approval template
Implement Local Induction for New Staff	On-going as and when new starters arrive. Data Custodians to provide IG handbook.		
Reporting IG Incidents and Breaches.	On-going as required. Report to IG Lead as and when events occur. Follow the Risk management process in all incidents		
Responding and Handling Subject Access Requests.	On-going as required. The Subject Access Request Register must be submitted to the Governance Officer on a bi-monthly basis.		
Information Sharing Protocols	On-going. Ensure IAO's & Project Leads are aware of the template and implement in new or existing projects.		
Data Protection Impact Assessments (DPIA)	On-going. Ensure IAO's & Project Leads are aware of the template and implement in new or existing projects.		

Appendix C –Data Security Protection Toolkit Assertions

Data Security and Protection Toolkit Assertions
There is senior ownership of data security and protection within the organisation.
There are clear data security and protection policies in place and these are understood by staff and available to the public.
Individuals' rights are respected and supported (GDPR Art 12-22)
Records of processing activities are documented for all uses and flows of personal information (GDPR Article 30 and Data Protection Act 2018 Schedule 1 Part 4)
Personal information is used and shared lawfully.
The use of personal information is subject to data protection by design and by default
Effective data quality controls are in place
There is a clear understanding and management of the identified risks to sensitive information and services
There is a clear understanding of what Personal Confidential Information is held.
Staff are supported in understanding their obligations under the National Data Guardian's Data Security Standards.
There has been an assessment of data security and protection training needs across the organisation.
Staff pass the data security and protection mandatory test.
Staff with specialist roles receive data security and protection training suitable to their role.
Leaders and board members receive suitable data protection and security training.
The organisation maintains a current record of staff and their roles.
Organisation assures good management and maintenance of identity and access control for its networks and information systems

All staff understand that their activities on IT systems will be monitored and recorded for security purposes.
You closely manage privileged user access to networks and information systems supporting the essential service
Process reviews are held at least once per year where data security is put at risk and following data security incidents
Participation in reviews is comprehensive, and clinicians are actively involved.
Action is taken to address problem processes as a result of feedback at meetings or in year.
A confidential system for reporting security breaches and near misses is in place and actively used.
All user devices are subject to anti-virus protections while email services benefit from spam filtering deployed at the corporate gateway.
Known vulnerabilities are acted on based on advice from CareCERT, and lessons are learned from previous incidents and near misses.
Organisations have a defined, planned and communicated response to Data security incidents that impact sensitive information or key operational services.
There is an effective test of the continuity plan and disaster recovery plan for data security incidents.
You have the capability to enact your incident response plan, including effective limitation of impact on your essential service. During an incident, you have access to timely information on which to base your response decisions.
All software has been surveyed to understand if it is supported and up to date.
Unsupported software and hardware is categorised and documented and data security risks are identified and managed.
Supported systems are kept up-to-date with the latest security patches.
You manage known vulnerabilities in your network and information systems to prevent disruption of the essential service
All networking components have had their default passwords changed.
A penetration test has been scoped and undertaken.
Systems which handle sensitive information or key operational services shall be protected from exploitation of known vulnerabilities.

You have demonstrable confidence in the effectiveness of the security of your technology, people, and processes relevant to essential services.
A data security improvement plan has been put in place on the basis of the assessment and has been approved by the SIRO.
You securely configure the network and information systems that support the delivery of essential services.
The organisation is protected by a well-managed firewall.
The organisation can name its suppliers, the products and services they deliver and the contract durations.
Basic due diligence has been undertaken against each supplier that handles personal information in accordance with ICO and NHS Digital guidance.
All disputes between the organisation and its suppliers have been recorded and any risks posed to data security have been documented.
All instances where organisations cannot comply with the NDG Standards because of supplier-related issues are recorded and discussed at Board.
The organisation understands and manages security risks to networks and information systems from your supply chain.

Appendix D – Training Needs Analysis 2019/20

Modules	Data Security Awareness Lv1 e-LfH modules	Data Security Awareness Lv1 ConsultOD link	The Role of the Caldicott Guardian - Workbook	Introduction to Risk Management for SIROs and IAOs
Senior Information Risk Owner	Mandatory To all new staff or contractors	Mandatory To all existing staff or contractors	Recommended	Mandatory
Caldicott Guardian	Mandatory To all new staff or contractors	Mandatory To all existing staff or contractors	Mandatory	Recommended
Data Protection Officer/Deputy Data Protetion Officer	Mandatory To all new staff or contractors	Mandatory To all existing staff or contractors	Recommended	Mandatory
Board & Lay Members	Mandatory To all new staff or contractors	Mandatory To all existing staff or contractors		Recommended
Information Asset Owners	Mandatory To all new staff or contractors	Mandatory To all existing staff or contractors		Mandatory
Data Custodians	Mandatory To all new staff or contractors	Mandatory To all existing staff or contractors		Recommended
All Staff	Mandatory To all new staff or contractors	Mandatory To all existing staff or contractors		

Colour code: **Complete once – Complete annually – Complete every 3 years**

Acknowledgement receipt

I confirm that:

I have received and read a copy of the Hampshire and Isle of Wight Partnership of CCGs Information Asset Owner and Data Custodian Handbook.

I accept and understand my role and responsibilities as (*delete as applicable) *Information Asset Owner/Data Custodian/Information Asset Assistant as set out in the Handbook.

Name: ……………………………………………………………………………..

Signature: …………………………………………………………………………

Job Title: ……………………………………………………………………………

Service: …………………………………………………………………………..

Date: ……………………………………………………………………………

Please return to the SCW Information Governance Team: **SCWCSU.IGEnquiries@nhs.net**