IG/03

Surrey Heartlands CCGs' Cyber and Information Security Policy

Policy applicable to:

NHS Guildford and Waverley CCG	✓
NHS North West Surrey CCG	✓
NHS Surrey Downs CCG	✓

Policy number	IG/03
Version	1.0
Approved by	CCG Senior Information Risk Owners
Name of originator/ author	Daniel Lo Russo, Head of Information Governance / Data Protection Officer
Owner	CCG Senior Information Risk Owners / ICS Directors
Date of last approval	March 2019
Next approval due	March 2020

Version control sheet

Version	Date	Author	Status	Comments / changes since last version
0.1	23/02/2019	Head of IG	Initial Draft	Reviewed by Data Protection Officer
0.2	06/03/2019	Head of IG	Approved by CCG IG Sub Committees	Minor amendments sec 7.23, 7.36 & 7.39 following review by IM&T Oversight Group
0.3	10/06/19	Corporate Governance	Draft	Appendix 1 amended
1.0	19/07/19	Head of IG	Final	Ratified by Audit Committees

The audience of this document should be aware that a physical copy may not be the latest version. The latest version, which supersedes all previous versions, is available via the CCGs' websites at link:

- NHS Guildford and Waverley Clinical Commissioning Group
- NHS North West Surrey Clinical Commissioning Group
- NHS Surrey Downs Clinical Commissioning Group

Equality statement

The Surrey Heartlands CCGs aim to design and implement services, policies and measures that meet the diverse needs of our service, population and workforce, ensuring that none are placed at a disadvantage over others. We take into account the Human Rights Act 1998 and promote equal opportunities for all. This document has been assessed to ensure that no employee receives less favourable treatment on the protected characteristics of their age, disability, sex (gender), gender reassignment, sexual orientation, marriage and civil partnership, race, religion or belief, pregnancy and maternity.

Members of staff, volunteers or members of the public may request assistance with this policy if they have particular needs. If the member of staff has language difficulties and difficulty in understanding this policy, the use of an interpreter will be considered.

We embrace the four staff pledges in the NHS Constitution. This policy is consistent with these pledges.

See next page for an Equality Analysis of this policy.

Equality analysis

Equality analysis is a way of considering the effect on different groups protected from discrimination by the Equality Act, such as people of different ages. There are two reasons for this:

- to consider if there are any unintended consequences for some groups
- to consider if the policy will be fully effective for all target groups

Name of Policy: Cyber & Information Security Policy	**Policy Ref:** IG/03	Is this New? [✓]
Assessment conducted by: Daniel Lo Russo, Head of IG / DPO		**Date of Analysis:** 15/03/2019
Directorate: Corporate Affairs and Governance	**Director's signature:** 	

1.	Who is intended to *follow* this policy? Explain the aim of the policy as applied to this group. See Scope – all individuals with access to the CCGs' to confidential / personal data or ICT systems which the CCGs are responsible for are required to comply fully with the requirements of this policy.
2.	Who is intended to *benefit from* this policy? Explain the aim of the policy as applied to this group. All CCG staff and users of CCG supplied or commissioned services will benefit from the CCGs complying with applicable legislation.
3.	**Evidence considered.** What data or other information have you used to evaluate if this policy is likely to have a positive or an adverse impact upon protected groups when implemented? • best practice and guidance shared via local and national networks; and • complaints made to CCGs.
a)	**Consultation.** Have you consulted people from protected groups? What were their views? We have not directly consulted CCG staff from protected groups. During 2019/20 the CCGs will establish a Patient Data Panel that will include people from protected groups and which will review IG related policies, procedures, data protection impact assessments, and information sharing agreements.
b)	**Promoting equality.** Does this policy have a positive impact on equality? What evidence is there to support this? Could it do more? Policy represents best practice.

c)	**Identifying the adverse impact of policies.** Identify any issues in the policy where equality characteristics require consideration for either those abiding by the policy or those the policy is aimed to benefit, based upon your research. Not applicable – reasonable adjustments will be made where required.
	i) People from different age groups: No adverse impact identified
	ii) Disabled people: Adverse impact identified – reasonable adjustments will be made where required (e.g. CCG will support people to make written requests for access to information or support for disabled staff members to access e-learning). Information supplied by the CCGs will meet the Accessible Information Standard.
	iii) Women and men: No adverse impact identified
	iv) Religious people or those with strongly help philosophical beliefs: No adverse impact identified
	v) Black and minority ethnic (BME) people: Potential adverse impact identified (people who do not have English as their first language) – reasonable adjustments will be made where required (e.g. CCG will support people to make written requests via translators etc.)
	vi) Transgender people: No adverse impact identified
	vii) Lesbians, gay men and bisexual people: No adverse impact identified
	viii) Women who are pregnant or on maternity leave: No adverse impact identified
	ix) People who are married or in a civil partnership: No adverse impact identified
4.	**Monitoring.** How will you monitor the impact of the policy on protected groups? The CCGs have in place established processes to gather complaints, compliments, and feedback from service users – relevant feedback to be reviewed by CCG Head of IG in liaison with Head of Engagement, Diversity & Inclusion and IG Sub Committees

Contents

1. Introduction and Policy Objective

1.1 Background

1.1.1 The purpose of cyber / information security is to ensure business continuity, to minimise the impact of incidents, and to ensure the integrity of the information and data held by the Surrey Heartlands CCGs.

1.1.2 This policy has been developed to ensure that the CCGs appropriately manage risks associated with cyber and information security. This will support the CCGs' compliance with the requirements of data protection related legislation, NHS Codes of Practice, and the NHS Data Security and Protection Toolkit as well as forming part of the CCGs' Business Continuity Management System (BCMS).

1.1.3 The purpose of this policy is to assist individuals undertaking work on behalf of the CCGs to conduct activity in a way that takes into account the applicable legislation, regulatory requirements, and best practice. This will support delivery of the CCGs' Strategic and Corporate Objectives (available at link).

1.1.4 The policy also reflects the underlying principles detailed in the CCGs' Information Governance Management Framework which are Accountability, Lawfulness, Fairness, and Transparency.

1.1.5 This is one of a suite of policies, procedures, and guidance material that link to the CCGs' Information Governance Management Framework (available at link). The policy reflects that the CCGs utilises a combination of locally managed information assets in addition to Information and communications technology (ICT) services provided by Commissioning Support Units (CSU) and other suppliers. The policy should be therefore considered alongside other documentation including CSU policies and system level security policies for specific information assets.

1.1.6 The policy reflects the current capacity, capability, and structure of CCGs and will be regularly reviewed to ensure that it remains aligned with these and fit for purpose.

1.1.7 This policy supersedes the following CCG specific policies:

CCG	Policy
NHS Guildford & Waverley CCG	Information Security Policy (59GB)
NHS North West Surrey CCG	Information Security Policy (IG04)
NHS Surrey Downs CCG	Information Security Policy (IG03)

2. Legislative Framework / Core Standards

2.1 Relevant Legislation

2.1.1 The policy reflects the requirements of the following key laws and legislation with which the CCGs are required to comply:

(1) Data Protection Act 2018 (DPA18). The purpose of this Act is to protect the rights and privacy of individuals. The DPA18 sets out six principles regarding how personal data should be used. The sixth principle of the DPA18 requires that personal data be processed in a secure manner.

(2) General Data Protection Regulation (GDPR). This is a legal framework that sets guidelines for the collection and processing of personal information of individuals within the European Union. The GDPR sets out the principles for data management and the rights of the individual, while also imposing significant fines for non-compliance.

2.2 Health & Social Care Specific Requirements

2.2.1 The below policy reflects the following health and social care sector specific statutory guidance with which the CCGs are required to comply.

2.2.2 The 'Information Security Management: NHS Code of Practice' is a guide to the management of information security, for those who work in or with NHS organisations in England. It's based on current legal requirements, relevant standards and professional best practice, and its guidelines apply to NHS information assets of all types.

3. Scope

3.1 Who this policy applies to

3.1.1 This policy applies to the Surrey Heartlands CCGs, which includes:

- NHS Guildford and Waverley Clinical Commissioning Group;
- NHS North West Surrey Clinical Commissioning Group; and
- NHS Surrey Downs Clinical Commissioning Group.

3.1.2 This policy applies to all permanent, contract or temporary staff of the CCGs and any third parties who have access to the CCGs' premises, systems or information.

3.1.3 Any reference to staff within this document also refers to those working on behalf of the organisation on a temporary, contractual, honorary, or voluntary basis.

3.2 What this policy applies to

3.2.1 This policy applies to:

- all information and data held and processed by the CCGs which must be managed and held within a controlled environment; including the personal data of patients and staff, as well as corporate information. It applies to information, regardless of format, and includes legacy data held by the organisation;
- information systems, data sets, computer systems, networks, software and information created, held or processed on these systems, together with printed outputs from these systems, and
- all means of communicating information, both within and outside the CCGs in both paper and electronic format, including data and voice transmissions, emails, post, fax, voice and video conferencing.

4. Definitions

4.1 Key Definitions

4.1.1 Information Security - ISO/IEC 27002:2013 describes information security in the following terms, which set the remit and principles behind this policy and related controls:

"Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or by using electronic means, shown on films, or spoken in conversation. Whatever forms the information takes, or means by which it is shared or stored, it should always be appropriately protected.

"Information security is the protection of information from a wide range of threats in order to ensure business continuity, minimise business risk, and maximise return on investments and business opportunities."

4.1.2 Information security has four key components:

- **Confidentiality**: assuring that sensitive information or data is accessible to only authorised individuals, and is not disclosed to unauthorised individuals or the public;
- **Integrity**: safeguarding the accuracy and completeness of information and software, and protecting it from improper modification;
- **Availability**: ensuring that information, systems, networks and applications as well as paper records are available when required to departments, groups or users that have a valid reason and authority to access them; and

- **Accountability**: ensuring that users are held responsible for their use of information.

4.1.3 Information security relates to both technical and physical data. It ranges from the security of networks, to the use of appropriate passwords by staff, and storage of confidential information in secure environments.

4.1.4 **Cyber Security** is concerned with the comprehensive risk management, protection and resilience of data processing systems and the digital networks that connect them. It is closely related to information security and mainly relates to processes involving data transferred or stored via the internet.

4.2 List of acronyms used in this policy

4.2.1 A list of abbreviations used within this document are included in the table below:

Term	Explanation
CSU	Commissioning Support Unit
DPA18	The Data Protection Act 2018
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
EPRR	Emergency Preparedness, Resilience and Response
GDPR	The General Data Protection Regulation
IAA	Information Asset Administrator
IAO	Information Asset Owner
ICO	Information Commissioner's Office
ICT	Information Communication & Technology
IG	Information Governance
IGSCs	Information Governance Sub Committees
IGMF	Information Governance Management Framework
IM&T	Information Management & Technology
SIRO	Senior Information Risk Owner

5. Roles and Responsibilities

Details of the key IG related roles within the Surrey Heartlands CCG' and their respective responsibilities are included within the Information Governance Management Framework. Specific roles and responsibilities with respect to this Policy are detailed below:

5.1 Commissioning Support Unit

5.1.1 NHS South, Central and West Commissioning Support Unit (SCWCSU) provide the Surrey Heartlands CCGs with ICT services and access to a

range of information assets; including clinical and technical applications, hardware, and other services. SCWCSU also provide Surrey Heartlands CCG's with specialist Information Security Manager support.

5.1.2 The SCWCSU provide Surrey Heartlands CCGs with regular assurance that the services supplied to the CCG comply fully with the Cyber and Information Security related elements of the NHS Data Security and Protection Toolkit and other applicable requirements.

5.2 The Governing Bodies

5.2.1 Individual CCG Governing Bodies are accountable for ensuring that the CCGs have an effective programme for cyber and information security assurance in place.

5.3 The Audit Committees

5.3.1 The CCG Audit Committees provide their respective Governing Body Committees with oversight for cyber and information security related matters. They therefore have responsibilities with respect to:

- being assured that this policy is, and remains, fit for purpose;
- the ratification of approval of this policy and associated work programmes; and
- considering regular summary assurance reports regarding the CCGs' compliance with the requirements of the policy.

5.4 The IG Sub Committees (IGSCs)

5.4.1 Each CCG has a dedicated committee to undertake detailed scrutiny of cyber and information security related activities. The IGSCs are sub-committees of the CCG Audit Committees.

5.4.2 The key roles and responsibilities of the IG Sub Committees of the CCGs are included within the Information Governance Management Framework available at link).

5.4.3 The IG Sub Committees have the following specific roles and responsibilities with respect to this policy:

- reviewing the policy and providing provisional approval of the policy and subsequent amendments to this for Audit Committees ratification;
- ensuring that appropriate cyber and information security related activities are included within the CCGs' annual IG Work & Improvement Programme;
- reviewing regular progress reporting with respect to the completion of cyber and information security related activities;

- setting and monitoring Key Performance Indicators with respect to cyber and information security related activities; and
- receiving reports regarding the CCGs' overall level of compliance with the requirements of this policy.

5.5 Corporate IM&T Oversight Group

5.5.1 The Corporate IM&T Oversight Group is an internal Surrey Heartlands CCGs working group that includes representation from: ICT, IG, EPRR, Facilities Management, and Business Support. They act as an advisory board for Corporate IM&T and ICT related projects and activities. They assist the CCGs in effectively managing cyber and information security related risks.

5.6 Joint Accountable Officer

5.6.1 The Joint Accountable Officer is ultimately responsible for ensuring that the Surrey Heartlands CCGs comply with cyber and information security requirements and manage associated risks appropriately.

5.7 Senior Information Risk Owner

5.7.1 The CCGs' Senior Information Risk Owners (SIROs) are the ICP Directors (secondment) within respective CCGs. Details of the key roles and responsibilities of the CCGs SIROs are detailed within the Information Governance Management Framework. Deputy SIRO's will be appointed and may fulfil the roles and responsibilities when the CCG's SIRO is unavailable.

5.7.2 SIROs / Deputy SIROs have the following specific roles and responsibilities with respect to this policy. They:

- have delegated responsibility for ensuring that the Surrey Heartlands CCGs comply with cyber and information security requirements;
- are the identified owner of the policy;
- approve any procedures related to this policy and changes to these;
- approve submission of the CCG's Data Security and Protection Toolkit;
- review and approve the CCG's Records of Processing;
- ensure that all individuals undertaking work for the CCGs complete mandatory Data Security Awareness training or equivalent;
- ensure that their CCG follows a 'data protection by design and default' approach in all activities;
- review and approve the outcomes of Data Protection Impact Assessments for activities where significant cyber and / or information security risks are identified;

- receive and review reports regarding the outcomes of Confidentiality Audits undertaken for their CCG; and
- ensure that suitable contracts or other agreements containing appropriate clauses relating to cyber and information security are in place with all individuals engaged to undertake work on behalf of their CCG.

5.8 The Caldicott Guardian

5.8.1 Each CCG has a Caldicott Guardian and their key roles and responsibilities are detailed within the Information Governance Management Framework. The Caldicott Guardians will provide advice and guidance regarding cyber and information security issues relating to heath records of NHS service users.

5.9 Information Asset Owners

5.9.1 The CCGs' have identified Information Asset Owners (IAOs) for all CCG Departments and Teams. IAOs are senior managers (e.g. 'Head of Function' or above). Details of the key roles and responsibilities of the CCGs SIROs are included within the Information Governance Management Framework.

5.9.2 They also have the following specific roles and responsibilities with respect to this policy. They:

- ensure that all information assets and flows of data to and from these are included within the Records of Processing for their team;
- provide approval of Records of Processing for their team and ensure that these are regularly updated;
- ensure that Data Protection Impact Assessments that are completed for their activities include assessments of related cyber and / or information security risks;
- ensure that records cyber and information security requirements relating to the information assets they are responsible for are detailed within System Level Security Policies;
- ensure that appropriate safeguards are in place for any information assets they are responsible for which include personal or confidential business data;
- undertake regular reviews of risks to confidentiality, integrity and availability of the information asset on a basis determined by the overall risk rating assigned to that asset; and
- provide the SIRO with assurance that information risks within their respective areas of responsibility are identified and recorded and that controls are in place to mitigate those risks.

5.10 Information Asset Administrators

5.10.1 CCGs' also have Information Asset Administrators (IAAs) who assist the IAOs to meet the responsibilities detailed above. IAAs support the development and update of Records of Processing for their teams and other cyber and information security related activities.

5.11 The Data Protection Officer

5.11.1 The CCGs are required to have a Data Protection Officer (DPO). Within SHCCGs this is the Head of Information Governance & Freedom of Information.

5.11.2 The key roles and responsibilities of the DPO are included within the Information Governance Management Framework. The DPO also has the following specific responsibilities with respect to this policy. They:

- ensure that this policy reflects legislative / NHS requirements and best practice;
- advise when Data Protection Impact Assessments may be required and review and approve the outcomes of these;
- provide the Joint Executive Team and Governing Bodies with regular reports regarding the CCGs' compliance with confidentiality and data protection related requirements.

5.12 The Surrey Heartlands CCGs' IG Team

5.12.1 The key roles and responsibilities of the CCGs' IG Team are included within the Information Governance Management Framework - they also have the following specific responsibilities with respect to this policy. They:

- They manage the process of ensuring that this policy and related procedures are kept up to date and aligned with the current capacity, capability, and structure of CCGs;
- manage the process for development and update of CCG Records of Processing;
- support teams to complete Data Protection Impact Assessments for their activities;
- support IAOs to develop System Level Security Policies which detail applicable cyber and information security requirements;
- undertake pre-award and post-award IG related assurance for CCG contracts;
- provide advice and guidance regarding how to securely handle and transfer personal data and confidential business data;

- undertake Confidentiality Audits, which include records management related checks, and provide reports regarding the outcomes of these;
- support internal and external reviews and audits of information quality;
- manage the CCGs' IG incident reporting process; and
- undertake checks of compliance with the requirements of this policy by individuals undertaking work on behalf of the CCGs and provide reports regarding these to the CCGs' SIROs and IG Sub Committees.

5.13 IM&T Programme Director

5.13.1 The Surrey Heartlands CCG IM&T Programme Director provides strategic support and guidance on Information Management & Technology (IM&T) related matters.

5.14 Directors and Managers

5.14.1 Directors and Managers of CCG Teams have the following specific responsibilities with respect to this policy. They:

- are required to ensure that all individuals undertaking work on behalf of their directorate / team comply fully with the requirements of this policy and related procedures;
- ensure that all individuals they are responsible for complete mandatory Data Security Awareness training;
- are responsible for ensuring that use of sponsored NHS Mail accounts complies with the NHS Mail Acceptable Use Policy;
- ensure that Data Protection Impact Assessments that are completed for their activities include assessments of related cyber and / or information security risks;
- ensure that contracts that relate to their area of the business are subject to pre-award and post-award IG related assurance;
- ensure that suitable contracts or other agreements containing appropriate clauses relating to cyber and information security are in place with all individuals / suppliers engaged to undertake work on behalf of the team;
- where cyber and information security issues are identified for activity they are responsible for, they ensure that appropriate mitigation is undertaken; and
- they receive and consider reports regarding the outcomes of Confidentiality Audits undertaken for their team's activities.

5.15 All staff and other individuals undertaking work on behalf of the CCGs

5.15.1 All staff and other individuals undertaking work on behalf of the CCGs contribute to cyber and information security and are responsible for any records that they create or use in the course of their duties. They are therefore required to:

- read this policy and understand how it relates to their role;
- comply fully with the requirements of this policy and related procedures;
- only handle and disclose personal data and confidential business data in accordance with requirements of applicable legislation, guidance, and this policy;
- assist fully with any cyber or information security reviews or audits of undertaken
- report any cyber or information security issues to the appropriate Information Asset Owner / Senior Manager; and
- report any breaches of the requirements of this policy to the CCGs' IG Team via the CCGs IG Incident Reporting process.

6. Procedures

6.1 Related Procedures

6.1.1 Procedures are the specific methods employed to express policies in action in day-to-day operations of the organisation. The following procedures are in place to assist individuals to comply fully with the requirements of this policy:

- Procedure for Handling Information Rights Related Requests (See Appendix 3 in Confidentiality & Data Protection Policy);
- IG Incident Management Procedure (See Appendix 2); and
- Data Protection Impact Assessment Procedure (See Appendix 5 in Confidentiality & Data Protection Policy);
- Secure Transfers of Data (see section 7.34 of the Information and Cyber Security Policy)

6.2 Supporting Guidance

6.2.1 Further supporting guidance is also available via the following:

- Information Asset Owners Handbook
- NHS Mail website

6.2.2 Or by emailing your query to the CCGs' IG Team at GWCCG.informationgovernance@nhs.net

7. Policy specific information

7.1 The National Data Guardian's Data Security Standards

7.1.1 The National Data Guardian's (NDG) Data Security Standards are particularly relevant to this policy:

(1) **Personal Confidential Data** – All staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form;

(2) **Staff Responsibilities** - All staff understand their responsibilities under the NDG's Data Security Standards, including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches;

(3) **Training** - All staff complete appropriate annual data security training and pass a mandatory test;

(4) **Managing Data Access** - Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All access to personal confidential data on IT systems can be attributed to individuals;

(5) **Process Reviews -** Processes are reviewed at least annually to identify and improve processes which have caused breaches or near misses, or which force staff to use workarounds which compromise data security;

(6) **Responding to Incidents** - Cyber-attacks against services are identified and resisted and CareCERT security advice is responded to. Action is taken immediately following a data breach or a near miss, with a report made to senior management within 12 hours of detection;

(7) **Continuity Planning** - A continuity plan is in place to respond to threats to data security, including significant data breaches or near misses, and it is tested once a year as a minimum, with a report to senior management;

(8) **Unsupported Systems** - No unsupported operating systems, software or internet browsers are used within the IT estate;

(9) **IT Protection** - A strategy is in place for protecting IT systems from cyber threats which is based on a proven cyber security framework such as Cyber Essentials. This is reviewed at least annually; and

(10) **Accountable Suppliers -** IT suppliers are held accountable via contracts for protecting the personal confidential data they process and meeting the National Data Guardian's Data Security Standards.

7.2 NHS Data Security and Protection Toolkit

7.2.1 The NHS Data Security & Protection Toolkit (available at link) is an online self-assessment tool that allows organisations to measure their performance against the National Data Guardian's 10 data security standards.

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

7.3 The CCGs' IG Work and Improvement Programme

7.3.1 The CCGs have an annual IG Work & Improvement Programme and this includes details of cyber and information security related activities that will be undertaken.

7.4 Training

7.4.1 The CCGs will complete an IG Training Needs Analysis on an annual basis and this will cover training requirements relating to confidentiality and data protection.

7.4.2 As a minimum, all individuals who have access to patient identifiable data or confidential business data will be required to complete mandatory NHS Data Security Awareness Training (or equivalent accredited training) on an annual basis.

7.4.3 Individuals will be notified of any other cyber and information security related training that is considered to be mandatory for their role.

7.5 Information Asset Registers

7.5.1 The CCGs will maintain and regularly review an Information Asset Register (IARs) that includes details relating to all Information Assets which are contain patient confidential data, special category staff personal data, or business critical business data. The IARs will be populated from Records of Processing.

7.6 Records of Processing

7.6.1 Data protection related legislation requires that all organisations hold, and can supply on request, detailed information regarding how it uses, shares, and holds personal data to supplement the summary information included within its Privacy Notice – these are known as it's Records of Processing (RoP).

7.6.2 All CCG teams will develop and maintain their own RoP-using the standard template in place with the CCGs. The key activities involved with completing the RoP are:

(1) Identifying and recording information assets; and

(2) Identifying and recording flows of data.

7.6.3 Team RoP should be reviewed and, if necessary updated, on at least an annual basis and at least every six months for areas of the business that handle patient data or sensitive staff data.

7.7 Managing Data Access

7.7.1 The CCGs will ensure that a range of controls are in place to manage data access and to restrict access to data to only those that require it for their current role. Access to information shall be restricted to users who have an authorised business need to access the information and as approved by the relevant IAO or Senior Manager.

7.7.2 Staff will be granted access to CCG information based on their role and to a level that will enable them to carry out their employment responsibilities. Regular reviews of access rights will be undertaken for or on behalf of the relevant IAO or Senior Manager.

7.8 Physical Access Controls

7.8.1 Confidential information will be physically protected from unauthorised access, damage, interference and/or alteration.

7.8.2 Information processing facilities will be housed in secure areas. These areas must be protected by defined security perimeters with appropriate security barriers and entry controls.

7.8.3 Confidential information will be physically protected from unauthorised access, damage, interference and/or alteration.

7.8.4 Information processing facilities will be housed in secure areas. These areas must be protected by defined security perimeters with appropriate security barriers and entry controls.

7.9 Equipment Security

7.9.1 In order to minimise loss of, or damage to, all assets that consist of ICT equipment above a specified monetary value shall be identified, registered and physically protected from threats and environmental hazards.

7.10 Role Based Access Control

7.10.1 The CCGs will implement Role Based Access Control (RBAC) to manage access to the electronic records stored within its electronic filing system

7.10.2 Regular reviews of user accounts for PCs / Laptops (Active Directory) and the RBAC assigned to these will be undertaken by senior managers within the CCGs with the assistance of the CCG Business Support Team and SCWCSU.

7.11 Access to CCG systems for individuals employed by other organisations

7.11.1 An appropriate agreement must be in place between the CCGs and the individuals – prior to access commencing this could be contract for services, honorary contract, or letter of authority. Please see the CCGs' Confidentiality and Data Protection Policy for further information. This requirement applies to the CCGs ICT systems, NHS Mail accounts, ICT equipment, phones etc. All users granted access must comply fully with any applicable Acceptable Use Agreements and System Level Security Policies.

7.12 Website (URL) Filtering

7.12.1 The CCGs and SCWCSU may restrict access to certain websites from CCG issued ICT equipment – if CCG users require access to a restricted website they should contact the CCGs' IG Team in the first instance. The CCGs' IG Team will assess the website and liaise with SCWCSU regarding whether this may be unrestricted.

7.13 Registration Authority

7.13.1 Please see the CCGs' Confidentiality and Data Protection Policy for further information regarding Registration Authority requirements.

7.14 Data Protection by Design and by Default

7.14.1 The CCGs shall implement appropriate organisational and technical measures to uphold the principles of data protection by design and by default from the beginning of any data processing and during the planning and implementation of any new data process.

7.14.2 The CCGs will integrate necessary safeguards to any data processing to meet regulatory requirements and to protect individual's data rights. This implementation will consider the nature, scope, purpose and context of any processing and the risks to the rights and freedoms of individuals caused by the processing.

7.14.3 Any new high-risk data processing activities will be assessed using a Data Privacy Impact Assessment (DPIA) before the processing commences. All new systems used for data processing will have data protection built in from the beginning of the system change.

7.14.4 All existing data processing has been recorded on the CCGs' Record of Processing. Each process has been risk assessed and is reviewed annually.

7.14.5 The CCGs will ensure that, by default, personal data is only processed when necessary for specific purposes and that individuals are therefore protected against privacy risks.

7.14.6 In all processing of personal data, the CCGs will use the least amount of identifiable data necessary to complete the work it is required for and will only keep the information for as long as it is required for the purposes of processing or any other legal requirement to retain it.

7.15 Accreditation

7.15.1 The CCGs will look for suppliers of ICT / IM&T related services to have one or more of the following accreditations:

- NHS Data Security and Protection Toolkit;
- ISO 27001 accreditation verified by audit; and
- Cyber Essentials Plus.

7.15.2 If these are not in place, the CCG may put in place additional contractual controls relating to cyber and information security to ensure that risks are appropriately managed by suppliers.

7.16 Data / Information Sharing Agreements

7.16.1 Data / Information Sharing Agreement utilised by the CCGs will detail applicable cyber and information security requirements. Please see the CCGs' Confidentiality and Data Protection Policy for further information regarding Data / Information Sharing Agreements.

7.17 Contact Assurance

7.17.1 The CCGs are required to ensure that formal contractual arrangements that include compliance with cyber and information security requirements are in place with all contractors and support organisations.

7.17.2 As an NHS Contracting Authority, the CCGs are responsible for obtaining appropriate pre and post award assurance with respect to compliance with IG requirements from all bodies that have access to the CCGs' information or conduct any form of information processing on their behalf, particularly where the information is about identifiable individuals or commercially sensitive.

7.18 Confidentiality Audits

7.18.1 The Data Security and Protection Toolkit requires that regular confidentiality audits are undertaken to check compliance with cyber and information security related requirements. Audits of all data processing facilities used by the CCGs and individuals undertaking working on our behalf may be undertaken by the CCGs' Information Governance Team.

7.19 Incident Management

7.19.1 The CCGs will ensure that any cyber or information security related incidents are managed, investigated, reported, and handled in accordance with NHS Digital's Guide to the Notification of Data Security and Protection Incidents - available at link.

7.19.2 Serious IG incidents will be reported to the Information Commissioner's Office and NHS Digital by the CCGs' IG Team using the NHS Data Security & Protection Toolkit within 72 hours of the CCG becoming reasonably aware that a serious incident has occurred.

7.19.3 A standard form for reporting IG incidents is available from the CCG websites at link below or is available from the IG Team via gwccg.information.governance@nhs.net:

- NHS Guildford and Waverley Clinical Commissioning Group;
- NHS North West Surrey Clinical Commissioning Group; and
- NHS Surrey Downs Clinical Commissioning Group.

7.19.4 Individuals should complete the form and forward this to CCGs' IG Team mailbox for processing.

7.19.5 The CCGs' IG Team will maintain a log of all reported / identified IG incidents.

7.19.6 Regular reports regarding cyber or information security related incidents will be provided to the CCGs' IG Sub Committees and Audit Committees.

7.19.7 The CCG will work with other organisations to ensure that lessons are learnt from any incidents and that actions are taken to minimise the occurrence of repeat of similar incidents.

7.19.8 IG incidents involving commissioned provider organisations or contracted suppliers will be reported to the relevant CCG Senior Manager and Contract Manager. Assurance with respect to commissioned provider organisations or contracted suppliers' management of IG incidents will be reviewed as part of standard CCG contract management processes.

7.19.9 Statutory disclosures relating to serious and reportable cyber or information security incidents will be included within the Governance Statements which form part of the CCGs' Annual Report & Accounts.

7.19.10 In line with the requirements of the NHS Standard Contract, the CCGs' On Call Managers will be notified of serious cyber or information security incidents involving Commissioned Providers and suppliers that occur outside of normal working hours and will support these organisations in ensuring that the incidents are managed, investigated, reported, and handled in accordance with NHS Digital's Guide to the Notification of Data Security and Protection Incidents.

7.20 CareCERT Alerts

7.20.1 NHS Digital provide a cyber and information security alert service on behalf of the NHS, known as CareCERT. SCWCSU manage CareCERT alerts relating to the ICT network the CCGs utilise and will provide the CCGs with regular assurance regarding the monitoring and mitigation of these.

7.21 Process Reviews

7.21.1 The CCG will undertake process reviews where repeat incidents have occurred. Process reviews will be documented and involve a range of stakeholders. Actions arising from process reviews will be agreed with the relevant Information Asset Owner / senior manager and reported to the SIRO.

7.22 Continuity Planning

7.22.1 The CCG will undertake regular Business Impact Assessments for its activities. These will include reviews of business continuity arrangements for key and critical information assets. Please see the CCGs' EPRR related policies for further information.

7.22.2 SCWCSU will provide assurance to the CCGs with respect to business continuity and disaster recovery arrangements in place for the information assets they are responsible for

7.23 Mobile Devices

7.23.1 Staff may use their own personal telephones / tablets to access NHS Mail in line with the NHS Mail Acceptable Use Agreement.

7.23.2 The Business Support Team will undertake regular reviews of the allocation of CCG managed devices and related accounts. Individuals are required to comply with the SCWCSU Mobile Device User Agreement which is applicable to the CCGs. Individuals are required to apply any security

updates as soon as possible after they are released if these are not applied automatically. Use of CCG issued devices must comply with this policy.

7.24 Laptops & Remote Access Solutions

7.24.1 The Business Support Team will undertake regular reviews of the allocation of CCG managed laptops and related remote access solution (RAS) accounts. Individuals' use of CCG issued devices must comply with this policy.

7.25 Unsupported Systems

7.25.1 The CCG will not allow the use of any unsupported ICT equipment or systems unless this has been approved by the SIRO in liaison with the IG Team, IM&T Programme Director, and, if relevant, SCWCSU.

7.26 IT Protection

7.26.1 The CCGs will ensure that appropriate technical controls are in place for ICT systems to minimise risks of inappropriate access to an acceptable level. The CCGs will ask system suppliers to provide assurance with respect to penetration testing undertaken for systems supplied to the CCGs.

7.26.2 The CCG, the CSU, and other system suppliers shall use software countermeasures and management procedures to protect itself against the threat of malicious software. All staff shall be expected to co-operate fully with this requirement and are required not to take any steps to bypass any protection.

7.26.3 Users shall not install software on the CCG / CSU ICT network / system without written permission from the CCGs' IG Team and/or SCWCSU. Users breaching this requirement may be subject to disciplinary action.

7.27 Virus Protection

7.27.1 The CCGs will ensure that virus protection is in place for ICT systems to minimise risks of inappropriate access to an acceptable level. The CCGS will ask system suppliers to provide assurance with respect to virus protection in place for systems supplied to the CCGs.

7.28 Password Protection

7.28.1 The SCWCSU Password Policy applies to Surrey Heartlands CCGs – this is included below.

7.28.2 Individuals are required to use complex passwords of a suitable length that are changed regularly and which include a combination of:

- upper and lower case letters; and

- symbols or numbers.

7.28.3 Passwords security is of critical importance and passwords must not be:

- easy to guess;
- written down; or
- shared with others.

7.29 System Level Security Policies and Controls

7.29.1 Key Information Assets that utilise information, usually referred to as Information Systems are required to have a System Level Policy that sets out their principles of operation and controls. Within these policies the approach to managing cyber and information security against the principles outlined in this policy are detailed.

7.29.2 These systems must consider the requirements of relevant legislation, legal gateways and national data standards; the policy outlines how they are incorporated and the relevant controls. Routine audits of controls on data and validation programmes are incorporated into system level policies and working practice and include:

- access control requirement specifications;
- authorisation process for access to the system (user registration and deregistration);
- assignment of responsibilities for the system (access, maintain and issue resolution);
- details on system design and dependencies, including encryption;
- provisions for reports generated by system utilities on use and audit logs;
- what system documentation is in place;
- login controls - threshold of failed logins;
- password controls;
- back-up requirements;
- back-up data testing arrangements;
- Business Continuity or back-up plans for system data and software applications;
- Details of UPS technologies or other system continuity support
- schedules of tests;
- input data validation;
- risk assessment for the system on key area;

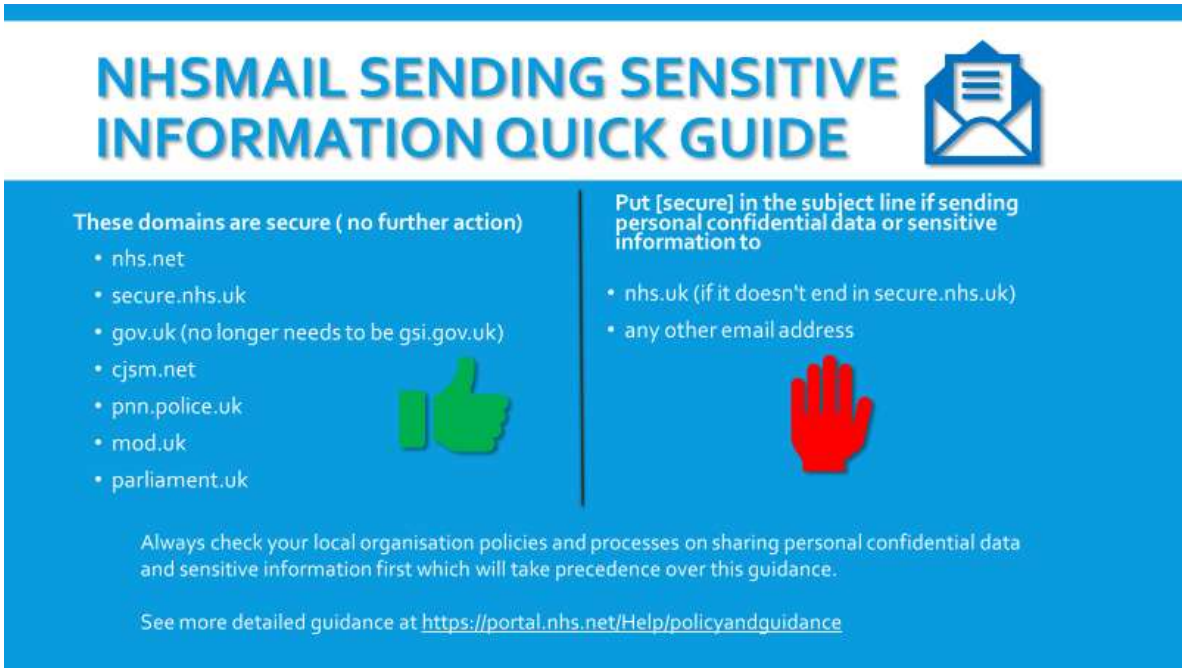
- policy detail on what security reports are available and who can provide them for the following issues, where appropriate;
- access log files generated by the system;
- current user overview;
- account monitoring (unused accounts etc.); and
- forensic readiness assessment.

7.29.3 Regular reviews of current controls and working practice are required to ensure that any developments of national standards and guidance. The standard and frequency for reviews will be outlined in the relevant System Level policy and as a minimum should be reviewed on at least an annual basis.

7.30 Email security

7.30.1 The CCGs will only use NHS Net Email for business communications. All individuals provided with access to an NHS Net account allocated to a CCG will be required to comply with the NHS Mail Acceptable Use Policy – available at **link.**

7.30.2 Individuals must also ensure that they use the NHS Net Encrypted email service as required – please see NHS Digital guidance "Sharing Sensitive Information by Email – A guide for Health and Social Care Organisations" and the diagram below for further information:



7.31 Sponsoring of NHS Net Email Accounts

7.31.1 CCGs may sponsor a small amount (e.g. maximum of five) NHS Mail accounts for organisations with which they have a need to securely transfer

patient confidential or sensitive business data. It is expected that providers of health and social care services put into place their own NHS Mail accounts or an alternative secure email service. SH CCGs will only be able to sponsor accounts for these types of organisations for a limited period of time, to be assed in line with business needs.

7.32 Port Control

7.32.1 The CCG may implement technical controls to restrict:

- ports for charging use only;
- the use of unencrypted devices; and
- devices that are not owned or managed by the CCG or CSU.

7.33 Use of encrypted devices / removable media

7.33.1 Individuals are prohibited from using unencrypted media to store any confidential business data or personal data held or used by the CCG. All USB sticks and other devices used to store patient confidential data must be encrypted up to AES256 bit standard or equivalent.

7.34 Secure transfers of confidential data

7.34.1 The CCGs will ensure that all transfer of confidential personal data are secure – this may include:

- via email encrypted to AES256 bit (see above);
- a staff member or suitably vetted third party transporting hard drive / remote storage device encrypted to AES256 bit level;
- NHS Secure File Transfer service;
- a secure file transfer undertaken by a CSU; and
- any other method agreed with CCGs' IG Team.

7.35 Accountable Suppliers

7.35.1 ICT suppliers will be held accountable for compliance with cyber and information security requirements via appropriate contract clauses being in place for the systems or services to be provided and regular assurance being received regarding these via the usual contract management process. The CCGs will seek to utilise standard NHS contracts for services in most cases. Contracts with ICT suppliers will include Data Processing Deeds as appropriate.

7.36 Assurance regarding use of CCG N3 / HSCN Connections

7.36.1 To assist with the effective delivery of health and social care services for NHS patients; the CCGs may allow other health and social care service provider organisations to use our trusted N3 link or connection to the successor Health and Social Care Network (HSCN). Any organisations that is allowed to utilise a CCG N3 / HSCN connection is required to provide assurance with respect to their usage of this and compliance with the requirements of the NHS Data Security and Protection Toolkit.

7.37 Surrey Community of Interest Network (COIN)

7.37.1 The CCGs utilise the Surrey Community of Interest Network (COIN) along with other health and social care service provider organisations. The CCGs will receive cyber and information security assurance from the organisations that are responsible for the management of the Surrey COIN and will be provided with details of any penetration testing or other audits undertaken for this network.

7.38 Remote Working

7.38.1 Individuals are required to ensure that their remote working practices comply with the cyber and information security requirements detailed within this policy. Please see further guidance included within the SH CCGs' Confidentiality and Data Protection Policy.

7.39 Forensic Readiness

7.39.1 Forensic Readiness is the ability of an organisation to maximise its potential to use digital evidence whilst minimising the costs of an investigation The CCGs will ensure that ICT systems and their usage support Forensic Readiness and this will:

- Protect the CCG, staff and clinical systems through the availability of reliable digital evidence gathered from its systems and processes;
- allow consistent, rapid investigation of major events or incidents with minimum disruption to CCG business;
- enable the pro-active and comprehensive planning, gathering and storage of evidence in advance of that evidence actually being required; and
- demonstrate due diligence and good governance of information assets.

8. Procedural requirements relating to this policy

8.1 Dissemination and Implementation

8.1.1 This policy and any subsequently approved versions will be distributed to staff via the CCG newsletter and placed on the CCG intranet. This policy will also be publicly available via the CCG websites.

8.1.2 All individuals undertaking work on behalf of the CCGs will be made aware of this policy during the induction process.

8.2 Process for Monitoring Compliance

8.2.1 The activities described in the CCGs' IG Work and Improvement Programme and supporting assurance plans will be used to monitor compliance with the requirements of this policy.

8.2.2 Individuals should be aware that their compliance with the requirements of this policy will be monitored by the CCGs via:

- regular confidentiality audits undertaken by the CCGs' IG Team;
- reviews of audit reports and other information relating to CCG systems which is supplied by SCWCSU, NHS Digital, and other suppliers;
- other reviews and audits commissioned by the CCGs.

8.2.3 Individuals should be aware that failure to comply with the CCGs' IG Management Framework and/or supporting policies may be dealt with as:

- a disciplinary matter in accordance with the CCGs' Human Resources related policies; or
- a breach of NHS Standard Terms and Conditions for the Supply of Services or other contract / agreement.

8.2.4 Serious non-compliance may also result in criminal proceedings being taken against the individual(s) involved.

8.3 Review Date

8.3.1 Review of this policy will take place on the first anniversary of adoption and subsequently every two years until rescinded or superseded. The review will be undertaken by the CCGs' Data Protection Officer.

9. Bibliography

9.1 Sources of information:

- Anonymisation: Managing Data Protection Risk Code of Practice at link
- General Data Protection Regulation at link
- 'Information Security Management: NHS Code of Practice'
- ICO website - link
- Information Governance Alliance GDPR Related Guidance at link.
- ISO/IEC 27002:2013 – Information Technology – see link
- NELCSU template CCG IG related policies
- NHS Digital's Guide to the Notification of Data Security and Protection Incidents available at link
- NHS Data Security & Protection Toolkit available at link
- NHS Digital guidance: Sharing Sensitive Information by Email – A guide for Health and Social Care Organisations - available at link
- NHS Mail website – available at link
- NHS South Central and West CSU ICT related policies
- Previous CCG policies and procedures
- Records Management Code of Practice for Health and Social Care 2016 at link
- UK legislation at link

10. Appendix 1 – Related Documents

This policy links to the following key documents:

Related policies

Other Surrey Heartlands CCG IG related policies as detailed below which are available at link:

- Information Governance Management Framework
- Confidentiality & Data Protection Policy
- Information Quality Policy
- Records Management Policy
- Public Access to Information and Re-Use Policy

In addition to the above the following policies of other organisations are also relevant

- NHS South Central and West CSU ICT Related Policies (available on request from the CCGs' IG Team via: GWCCG.informationgovernance@nhs.net)

IG related procedures

This policy links to the following key IG related procedures:

- Procedure for Handling Information Rights Related Requests (See Appendix 3 in Confidentiality & Data Protection Policy);
- IG Incident Management Procedure (see appendix 2); and
- Data protection Impact Assessment Procedure (see appendix 3)
- Secure Transfers of Data (see section 7.34 of the Information and Cyber Security Policy)

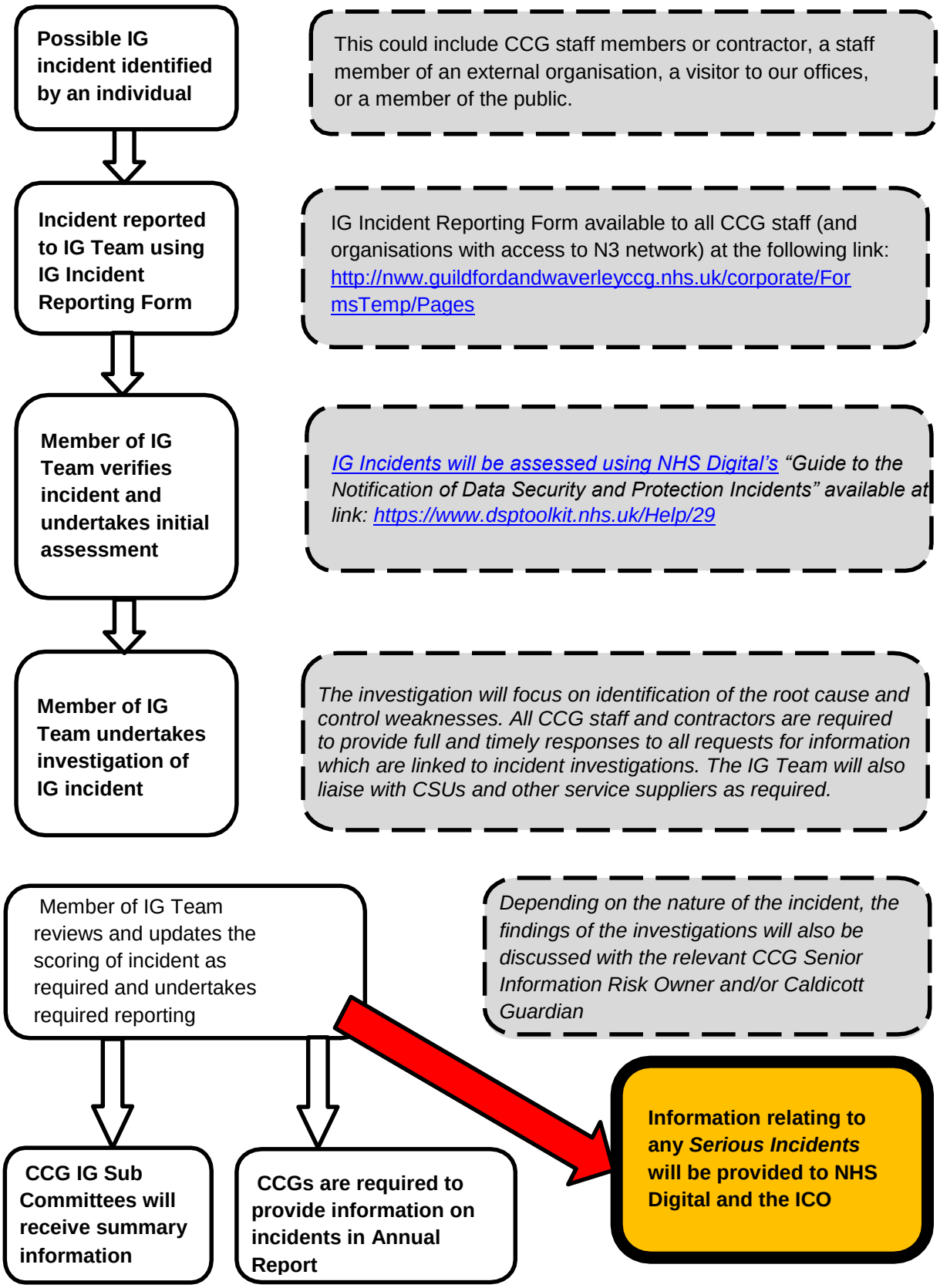
Guidance Documents

Further guidance is also available via the information governance team:

- What you need to know about IG: and
- Information Asset Owners Handbook.

11. Appendix 2 – IG Incident Management Procedure

Stage 1 – Identification and investigation of IG Incidents: *The CCGs aim to complete the steps below within 24 hours for serious incidents and 5 working days for other IG incidents.*



Step 1 - Identification of an Incident

An IG incident can include any breach of the CCGs' IG related policies, applicable legislation, or NHS requirements. IG incidents can therefore include a diverse range of situations including:

- lost staff identity badge or desk pedestal keys;
- mislaid document including confidential information;
- access to patient identifiable data by someone who does not have a need to know;
- lost or stolen CCG issued lap-top, mobile phone, or USB drive; and
- hacking of electronic data or attack by a computer virus or other malicious software

The CCGs' values include openness and honesty and the CCGs therefore encourage individuals to immediately report any suspected or actual IG incidents, so these can be investigated if required. This enables the CCGs to identify any control weaknesses and put in place remedial action to reduce the likelihood of similar incidents occurring going forward.

IG incidents can be identified by CCG staff, staff of partner organisations, suppliers, visitors to the CCG's offices, and members of the public. The CCG may receive notification of an incident verbally, by email, in a letter or other means. The CCG staff member who is first contacted should ensure that the incident is reported using the CCG's IG Incident Reporting Form in accordance with these procedures.

An IG Incident Reporting Form is available to all CCG staff (and organisations with access to the N3 network) at the 'Forms and Templates' section (Corporate > Forms & Templates) of the CCG's Intranet at the link below:

The Incident Reporting Form captures the following key information:

- details of the individual who identified the incident;
- details of the individual who reported the incident;
- a description of the incident;
- any relevant background information;
- the date the incident was identified; and
- the date the incident was reported.

The partially completed form should be sent in Word version by email to the contact details provided on the form so this can be received by the CCGs' Information Governance Team. All incidents should be reported to the IG Team on the business day they are identified.

Step 2- Initial Assessments

A member of the IG Team will complete an initial assessment of the incident and this will be completed within 24 hours or receipt of an IG Incident Form and ideally on the same business day as it is received.

Using the information provided on the form (and if necessary discussion with the individual(s) who identified or reported the incident) the member of the IG Team will make an in initial assessment including:

- whether an IG incident has taken place;
- likely Incident Scale (e.g. near miss, IG incident, Serious IG Incident); and
- any immediate remedial actions required to contain incident and minimise impact.

The member of the IG Team will then assess the scale and impact of the incident using the applicable criteria, which include:

- incident type categorisation (e.g. how incident occurred);
- baseline (e.g. number of individuals the data relates to);
- low sensitivity factors (e.g. whether information is unlikely to identify an individual or already otherwise available); and
- high sensitivity factors (e.g. whether the information is particularly sensitive and whether the individual it relates to or the organisation is now put at significant risk).

Based on the above the incident will be given an indicative score and a decision made by the IG Team as to any further action required, which can include:

- no further action – appropriate remedial action has been identified and can easily be taken to reduce likelihood of incident recurring (score is confirmed); or
- further action required – investigation required to identify appropriate remedial action and fully assess scale and impact of incident and confirm scoring.

Step 3 - Investigation of Incidents

In accordance with the targets in applicable guidance, the CCGs will look to fully complete the investigation of possible Serious IG Incidents (and undertake any initial external reporting that may be required) as soon as possible and ideally within 24 hours of the incident being identified. The ICO and Department of Health will be notified of any serious incidents within 72 hours of the CCG verifying that a serious incident has occurred.

It is expected that the CCG will fully complete investigations required for other IG incidents (and undertake any initial external reporting that may be required) as soon as possible and ideally within five working days of the incident being verified.

All CCG staff and contractors are therefore required to provide full and timely responses to all requests for information which are linked to incident investigations.

As part of the investigation the IG Team will consult with stakeholders and liaise with providers of commissioning support services as required.

The IG Team will then update the IG Incident Report Form to include details of:

- root cause analysis;
- identified control weakness;
- remedial actions undertaken;
- recommendation for any further remedial action required (such as informing data subjects); and
- lessons learnt

The indicative score will be reviewed and revised as required and a recommendation made as to any further action required, which can include:

- if the incident requires local reporting only;
- if the incident is a serious incident requiring external reporting to NHS Digital and ICO via the NHS Data Security and Protection Toolkit.

The CCG's Senior Information Risk Owner will approve the outcomes of the investigation. They may seek advice and guidance from the CCG's Caldicott Guardian where incidents relate to personal data and, particularly, when incidents relate to sensitive personal data of Guildford and Waverley patients.

The IG Team will maintain an audit trail of events and evidence supporting decisions taken during the incident investigation. In the case of incidents that require further investigation, the data the incident relates to will be securely held by the IG Team or SIRO/Caldicott Guardian until the investigation has been completed.

Step 4 - Reporting of Incidents

The IG Team will liaise with NHS Digital and ICO with respect to Serious Incidents. The SIRO will be kept informed with respect to progress with implementing the remedial actions agreed for Serious Incidents and will provide updates at the Joint Executive Team meetings as required.

The IG Team will ensure that incidents are reported as follows:

Where	IG Sub Committees	To NHS Digital and ICO via DSP Toolkit	Annual Report & Accounts
What	Summary information on all IG incidents and near-misses	Information relating to Serious Incidents	Detailed information relating to Serious IG Incidents Summary information relating to other incidents
When by	Three times per annum	ASAP and ideally within 24 hours of being confirmed	Annual

12. Appendix 3 – Data Protection Impact Assessment Procedure

Introduction

To ensure that a data protection by design and default approach is followed the following data protection impact assessment procedure will be in place at the CCGs.

The Information Commissioner's Office defines a Data Protection Impact Assessment (DPIA) as: '*… a process designed to help organisations systematically analyse, identify and minimise the data protection risks of a project or plan. It is a key part of the organisations accountability obligations under the GDPR, and when done properly helps assess and demonstrate how to comply with all data protection obligations. It does not have to eradicate all risk, but should help minimise and determine whether or not the level of risk is acceptable in the circumstances, taking into account the benefits of what you want to achieve*.'

A DPIA is a tool that supports proper planning for the effective implementation of new or changed systems in a way that assures the confidentiality, security and integrity of personal data and confidential business data.

Under the GDPR, failure to conduct a DPIA that is likely to result in a high risk to the rights and freedoms of individuals, could lead to enforcement action, a fine of up to €10 million, or 2% global annual turnover if higher.

Scope

This procedure applies to:

- all staff of the Surrey Heartlands CCGs and other individuals undertaking work on the CCGs' behalf; and
- all processes that include a new or changed use of Personal Confidential Data (PCD) and/or Business sensitive data in any format.

Typical examples of when a DPIA is required include:

- introduction of a new paper or electronic information system to collect and hold personal/business sensitive data;
- introduction of a new service or a change to existing process, which may impact on an existing information system;
- update or revision of a key system that might alter the way in which the CCGs' use, monitor, and report personal/business sensitive information;
- replacement of an existing data system with new software;
- changes to an existing system where additional personal/business sensitive data will be collected;
- plans to outsource business processes involving storing and processing personal/business sensitive data;
- changes to 'data processing facilities' including CCG offices where staff handle PCD; and
- any change to or introduction of new data / information sharing agreements.

Process

A DPIA should begin at the start of any project to run alongside the planning and development process. It should include these steps:

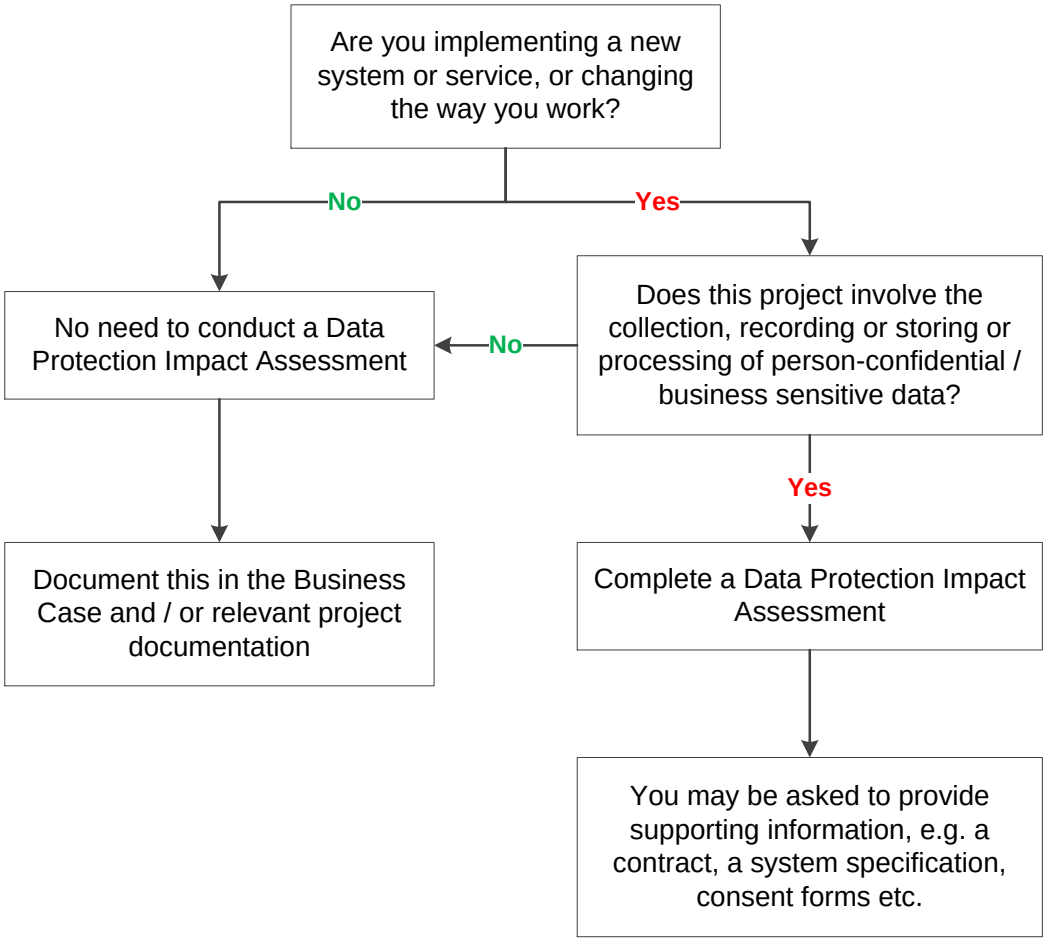
- Step 1: identify the need for a DPIA;
- Step 2: describe the processing;
- Step 3: consider consultation;
- Step 4: assess necessity and proportionality;
- Step 5: identify and assess risks;
- Step 6: identify measures to mitigate the risks;
- Step 7: sign off and record outcomes;
- Step 8: integrate outcomes into plan; and
- Step 9: keep under review.

Step 1 – Identification

The CCGs will utilise a range of methods to identify where DPIAs are required:

- the CCGs' Head of IG and Data Protection Officer will review the CCGs' commissioning intentions and departmental business plans etc. to identify activities for which a DPIA is likely to be required;
- on a quarterly basis, the IG Team will email all Information Asset Owners to ask them to provide details of any forthcoming new activities which involve the processing of personal data or proposed changes to existing processes; and
- at all other times IAOs and other individuals should provide notification of any forthcoming new activities which involve the processing of personal data or proposed changes to existing processes by making the CCGs' IG Team aware of these (details of proposed new activities should be sent to the IG Team generic mailbox).

The diagram below may assist in indicating when a DPIA is required however Teams are encouraged to confirm the requirement with the CCGs' IG Team.



Step 2 – Describe the Processing

DPIAs completed by the CCGs will adequately describe the nature, scope, context and purposes of the processing.

They will set out clearly the relationships between controllers, processors, data subjects and systems, using both text and data-flow diagrams where appropriate.

DPIAs should explicitly state how the CCG(s) will comply with each of the Data Protection Principles under GDPR and clearly explain the lawful basis for processing (and special category conditions if relevant).

DPIAs will also explain how the CCG(s) plan to support the relevant information rights of its data subjects.

DPIAs should be written in plain English, with a non-specialist audience in mind, explaining any technical terms and acronyms used.

Step 3 - Consultation

The CCGs will undertake adequate consultation when completing DPIAs and this should include:

- advice from the Data Protection Officer (DPO) and discussion with members of the CCGs' IG Team;
- asking any data processors to help us understand and document their processing activities and identify any associated risks; and
- directly consulting individuals (or their representatives) and other relevant stakeholders.

Completed DPIAs will provide details of any stakeholder consultation undertaken and include summaries of findings.

Step 3 - Assessing necessity and proportionality

As part of the DPIA the CCGs will check that the processing is necessary for and proportionate to its purposes, and describe how it will ensure compliance with data protection principles.

Step 5 – Identification and assessment of risks

DPIAs completed by the CCGs will include an objective assessment of the likelihood and severity of any risks to individuals' rights and interests.

Completed DPIAs will have identified all relevant risks to individuals' rights and freedoms, assessed their likelihood and severity, and detailed all relevant mitigations.

Step 6 - Identification of measures to mitigate the risks

The DPIAs will identify measures that can put in place to eliminate or reduce high risks. DPIAs will explain sufficiently how any proposed mitigation reduces the identified risk in question.

DPIA will also evidence consideration of any less risky alternatives to achieving the same purposes of the processing, and why it didn't choose them.

The CCGs will consult the ICO before processing, if it cannot mitigate high risks.

Step 7 - Sign off and record outcomes

DPIAs will include details of any advice and recommendations provided by the DPO.

The CCGs will record its decision-making in the outcome of the DPIA, including any difference of opinion with its DPO or individuals consulted.

The DPIA will be signed off by the appropriate person within the relevant CCG(s). Formal sign off for DPIAs is as follows and must be obtained in writing:

Overall risk level	Approval
DPIA includes one of more identified risks with overall risk level of high or above post-mitigation	Senior Information Risk Owner / Deputy or Caldicott Guardian

DPIA includes no risks with overall risk level of high or above post-mitigation	Information Asset Owner or Director / Deputy Director

Step 8 - Integrate outcomes into plan

Information Asset Owners and Senior Managers with the CCGs are responsible for implementing the measures identified in the DPIAs and ensuring that there are integrated into the project plan.

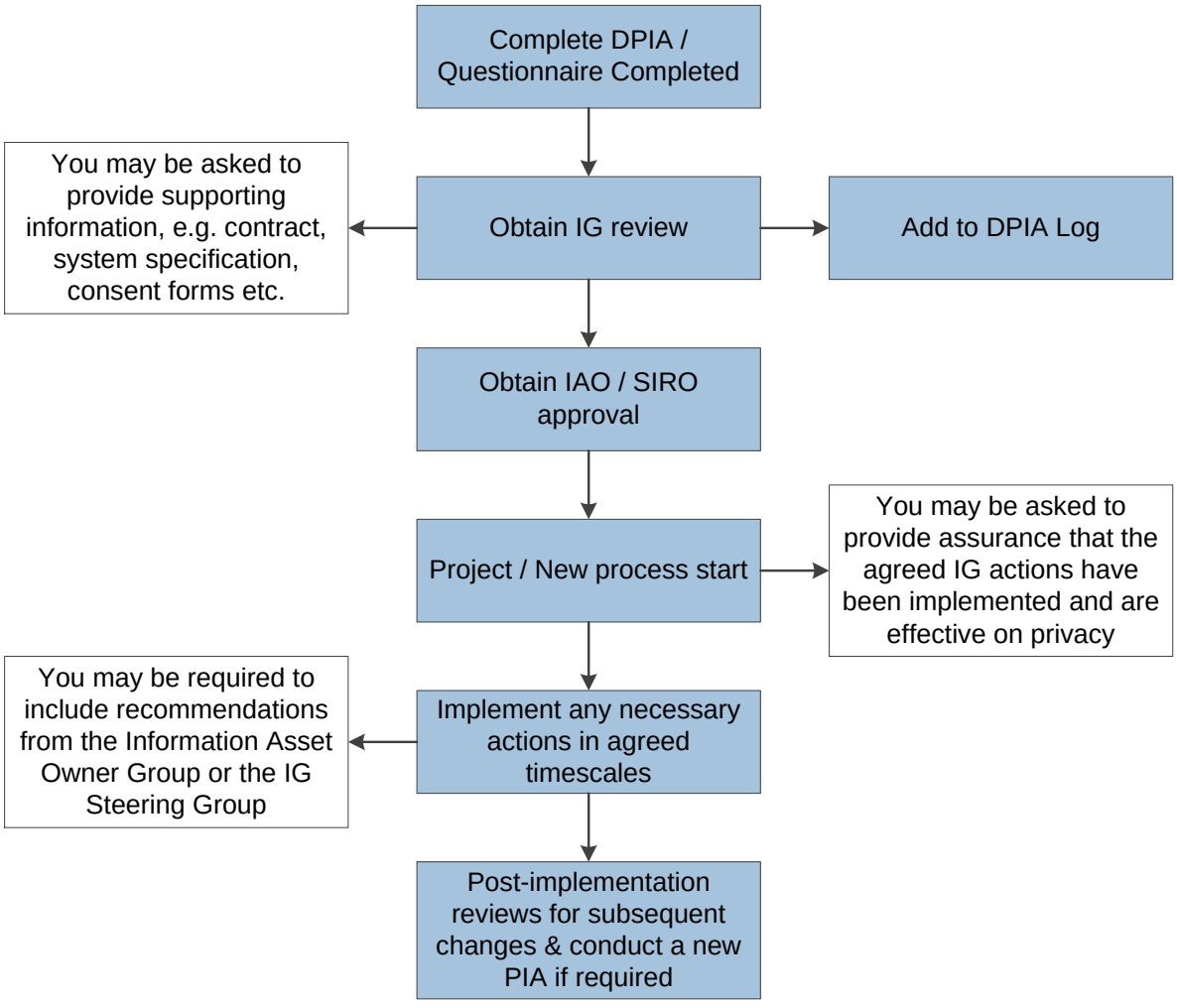
Step 9 - Keep under review

The CCGs will keep DPIAs under review and revisit them when necessary. Completed DPIAs will include a schedule for reviewing the DPIA regularly or should be reviewed when there is any significant change to the nature, scope, context or purposes of the processing.

The CCGs' IG Team may undertake audits to check that measures identified within DPIAs have been fully implemented and are effective in mitigating risks.

Summary of process for DPIAs

The diagram below provides a summary of the process for completing DPIAs within the Surrey Heartlands CCGs:



13. Appendix 4 - Procedural Document Checklist for Approval

Title of document being reviewed:		Yes/No/ Unsure	Comments/Details
A	**Is there a sponsoring director?**	Yes	ICS Director of Corporate Affairs and Governance
1.	**Title**		
	Is the title clear and unambiguous?	Yes	
	Is it clear whether the document is a guideline, policy, protocol or standard?	Yes	Policy
2.	**Rationale**		
	Are reasons for development of the document stated?	Yes	Comply legislation and DSPT
3.	**Development Process**		
	Do you feel a reasonable attempt has been made to ensure relevant expertise has been used?	Yes	
	Is there evidence of consultation with stakeholders and users?	Yes	Reflects best practice
4.	**Content**		
	Is the objective of the document clear?	Yes	
	Is the target group clear and unambiguous?	Yes	
	Are the intended outcomes described?	Yes	
5.	**Evidence Base**		
	Is the type of evidence to support the document identified explicitly?	Yes	
	Are key references cited?	Yes	
6.	**Approval**		
	Does the document identify which committee/group will approve it?	Yes	
7.	**Dissemination and Implementation**		
	Is there an outline/plan to identify how the document will be disseminated and implemented amongst the target group? Please provide details.	Yes	
8.	**Process for Monitoring Compliance**		
	Have specific, measurable, achievable, realistic and time-specific standards been detailed to monitor compliance with the document? Complete Compliance & Audit Table.	Yes	
9.	**Review Date**		
	Is the review date identified?	Yes	

Title of document being reviewed:		Yes/No/ Unsure	Comments/Details
10.	**Overall Responsibility for the Document**		
	Is it clear who will be responsible for implementing and reviewing the documentation i.e. who is the document owner?	Yes	
ICP Director Approval			
On approval, please sign and date it and forward to the chair of the committee/group where it will receive final approval.			
Name	Vicky Stobbart	Date	15/03/19
Signature			
Name	Karen Thorburn	Date	15/03/19
Signature			
Name	Colin Thompson	Date	15/03/19
Signature			
Audit Committee Approval			
On approval, Chair to sign and date.			
Name	Jacqui Burke	Date	19/07/19
Signature			

14. Appendix 5 - Compliance and Audit Table

Criteria	Measurable	Frequency	Reporting to	Action Plan/ Monitoring
Non-compliance with the requirement of this policy	No. of occurrences, target zero	Quarterly	Information Governance Sub Committees	2018/19 IG Work & Improvement Programme Regular confidentiality audits
Serious cyber and information incidents externally reported within 72 hours	Number and time take to report, target 100%	Quarterly	Information Governance Sub Committees	2018/19 IG Work & Improvement Programme IG Incident Log
Data Protection Impact Assessments (DPIAs) completed include cyber and info security requirements	Whether DPIA completed includes requirement	Quarterly	Information Governance Sub Committees	2018/19 IG Work & Improvement Programme DPIA Log
System Level Security Policies completed include cyber and info security requirements	Whether DPIA completed includes requirement	Quarterly	Information Governance Sub Committees	2018/19 IG Work & Improvement Programme DPIA Log
Independent auditor review of compliance with the NHS Data Security & Protection Toolkit	Overall audit opinion (target reasonable) and number of final recommendations (target < 5).	Annual	Information Governance Sub Committees	2018/19 IG Work & Improvement Programme Audit Planning Memorandum