INFORMATION ASSURANCE DOCUMENTED PLAN:

Document History

Document Reference:	IG18
Version:	Revised Policy
Ratified by:	SL/SWL CCG Governing Bodies
Date ratified	March 2018
Name of originator/author	Information Governance Services
Name of responsible committee/individual:	Senior Leadership Team
Date issued:	March 2018
Review Date:	February 2021
Target audience:	All Staff within the CCG whether operating directly or providing services to other organisations under a service level agreement or joint agreement and to none executive directors, contracted third parties (including agency staff), locums, students, volunteers, trainees, visiting professionals or researchers, secondees and other staff on temporary placements within the organisation.
Distributed via:	Website
Document Purpose:	This document sets out the procedure to ensure that all information assets are identified and regularly assessed to ensure the confidentiality and security of the organisations' information is maintained.

South Lincolnshire CCG
South West Lincolnshire CCG

CONTENTS

V**ersion control sheet**

Version	Section/Para/Appendix	Version/Description of Amendments	Date	Author/	Version
Revised Version Serving SL and SWL CCGs (dual branding)	Policy Review	Incorporates specific reference to impending General Data Protection Regulation (Revised as a dual branded policy for NHS South Lincolnshire CCG and NHS South West Lincolnshire CCG) Replaces existing policies within SL and SWL CCG referenced IG18.	27/02/2018	JE	1

ASSISTANCE WITH THE APPLICATION OF THIS POLICY AND UPDATES

This policy has been prepared so as to reflect the law as at 14 February 2018. The policy will require periodic review to reflect subsequent changes to the law. Under the General Data Protection Regulation (GDPR) (which will apply from 28th May 2018), personal data must be processed in accordance with certain principles. While these are broadly similar to those under the Data Protection Directive (DPD), the wording has changed and they all centre around the concept of accountability.

The GDPR applies to 'controllers' and 'processors'; A controller determines the purposes and means of processing personal data whilst a processor is responsible for processing personal data on behalf of a controller. If you are a processor, the GDPR places specific legal obligations on you; for example, you are required to maintain records of personal data and processing activities. You will have legal liability if you are responsible for a breach. However, if you are a controller, you are not relieved of your obligations where a processor is involved – the GDPR places further obligations on you to ensure your contracts with processors comply with the GDPR. The General Data Protection Regulations (GDPR) (Regulation (EU) 2016/679) – is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union. GDPR applies to those who have a day to day responsibility for data protection. This should be read in conjunction with the CCGs' Information Governance Staff Handbook.

1. Introduction and aims

The purpose of this document is to provide guidance to all NHS South Lincolnshire and NHS South West Lincolnshire Clinical Commissioning Groups' (CCG) staff on the CCG's Information Assurance Documented Plan

.

The aims of this document are to ensure that:

- Individuals are aware of the support necessary to ensure work related to information security management is appropriately carried out
- Individuals are aware of the CCG's mandatory responsibilities in relation to information security management issues and their own responsibilities.

2. Scope

This policy applies to those members of staff that are directly employed by the CCG and for whom the CCG has legal responsibility. This policy applies to all third parties and others authorised to undertake work on behalf of the CCG.

3. Information Assurance Documented Plan

This documented plan for Information Assurance Documented Plan headed up by the Senior Information Risk Owner (SIRO), identifies the support necessary to ensure work related to information security management is appropriately carried out.

The information assurance documented plan details:

- The promotion of information security throughout the Clinical Commissioning Group.
- The review and recommendation for the approval of all information security related policies and procedures.
- The monitoring of progress in programmes to achieve compliance/certification with ISO27001.
- The review and monitoring of security incidents, their cause, resolution and future prevention.
- Reviewing information security risk assessments and improvement plans.
- Consideration of solutions to improve security.
- Monitoring and auditing compliance with standards and policies.
- Receiving and reviewing information security related reports (e.g. internal audit)
- Reviewing and commenting upon the security impact of information system development.
- Reviewing, and recommending for approval, the information security elements of the annual IG toolkit submission.

4. Accountability

Overall responsibility for the Information Assurance Plan sits with the Accountable Officer who has delegated the responsibility for managing the Plan to the Senior

Information Risk Owner in the CCG. Support is provided from the OPTUM Commissioning Support Services Information Governance Team under contractual terms.

The CCG may take disciplinary action against users found to have contravened this Plan.

5. Training

Mandatory Data Security Awareness Training to be completed by all staff via ESR.

6. Equality and Diversity

The CCG aims to design and implement policy documents that meet the diverse needs of the services, population and workforce, ensuring that none are placed at a disadvantage over others. It takes into account current UK legislative requirements, including the Equality Act 2010 and the Human Rights Act 1998, and promotes equal opportunities for all.

This document has been designed to ensure that no-one receives less favourable treatment due to their personal circumstances, i.e. the protected characteristics of their age, disability, sex (gender), gender reassignment, sexual orientation, marriage and civil partnership, race, religion or belief, pregnancy and maternity. Appropriate consideration has also been given to gender identity, socio-economic status, immigration status and the principles of the Human Rights Act.

In carrying out its functions, the CCG must have due regard to the Public Sector Equality Duty (PSED). This applies to all the activities for which the Clinical Commissioning Group is responsible, including policy development, review and implementation.

7. Due Regard

This policy has paid due regard to the Public Sector Equality Duty (PSED) of the Equality Act 2010 to eliminate discrimination, harassment, victimisation; to advance equality of opportunity; and foster good relations.

8. Review

This plan will be reviewed annually in line with Information Governance Toolkit requirements or where changes occur with legislation or national policy.

Appendix 1 - Equality Analysis Initial Assessment

Title of the change proposal or policy:

Information Assurance Documented Plan

Brief description of the proposal:

To ensure that the policy amends are fit for purpose, that the policy is legally compliant, complies with legislative requirements and includes details of the European Directive – General Data Protection Regulations.

Name(s) and role(s) of staff completing this assessment:

June Emptage – Information Governance Officer

Date of assessment: 27 February 2018

proposed change:

Will it affect employees, customers, and/or the public? Please

state which.

Yes it will affect all employees and those who enter into contractual arrangements with the organisation.

Is it a major change affecting how a service or policy is delivered or accessed?

No – although it introduces new General Data Protection Regulations which will be mandatory in May 2018

Will it have an effect on how other organisations operate in terms of equality?

No

If you conclude that there will not be a detrimental impact on any equality group, caused by the proposed change, please state how you have reached that conclusion:

No anticipated detrimental impact on any equality group. The policy adheres to the legislative requirements which are applicable to all.