STELLAR
HEALTHCARE

Information Governance Policy

Policy Summary

This policy outlines the organisation's approach to the management of Information Governance and information handling. It explains the accountability and reporting arrangements for Information Governance and how assurance is provided to meet at least the minimum standards of Information Governance compliance required by the NHS Information Governance Toolkit

Version	Date Issued	Details	Brief Summary of Change	Author
0.1	20/05/2014	Draft	New document	NHS Central Eastern Commissioning Support Unit - Information Governance Team
1.0	18/06/2014	Final	Approved	NHS Central Eastern Commissioning Support Unit - Information Governance Team
2.0	23/09/2016	Review	No significant change	
3.0	23/09/2018	Review	GDPR Compliancy	
3.1	18/10/2020	Review		

Compliance with all Stellar Healthcare policies, procedures, protocols, guidelines, guidance and standards is a condition of employment. Breach of policy may result in disciplinary action.

Version control

For more information on the status of this policy, please contact:	
NHS Central Eastern Commissioning Support Unit	Information Governance Team
Approved by	Stellar Healthcare Board
Approval Date	18/10/2020
Next Review Date	17/10/2023
Responsibility for Review	Stellar Healthcare
Contributors	Stellar Healthcare IG Lead, SIRO, Caldicott Guardian
Audience	All Stellar Healthcare officers and staff (which includes temporary staff, contractors and seconded staff).

Contents

1. Introduction

Information Governance (IG) is a combination of legal requirements, policies and best practice designed to ensure all aspects of information processing and handling are of the highest standards.

IG requirements have been traditionally addressed within the NHS by separate work streams covering the following areas:

- Confidentiality and Data Protection
- Information Security
- Records Management (including corporate and clinical records)
- Data Quality
- Records Management

Information is a vital asset, both in terms of the clinical/corporate management of individual patients/service-users/staff and the efficient management of services and resources. It plays a key part in corporate/clinical governance, service planning and performance management.

It is therefore of paramount importance to ensure that information is effectively managed and that appropriate policies, procedures and management accountability and structures are in place to provide a robust governance framework for information management. Within the NHS this aspect of information management is termed Information Governance.

This document sets out the approach to be taken by Stellar Healthcare to provide assurance on how that personal information will dealt be with legally, securely, efficiently and effectively, in order to deliver the best possible care and service.

2. Scope

Information Governance is formed by those elements of law and policy, from which applicable information governance standards are derived. It encompasses legal requirements, central guidance and best practice in information handling including:

- Data Protection Act 1998
- Freedom of Information Act 2000
- The Common Law of Duty and Confidentiality
- Information Quality
- Records Management
- Caldicott Principles

This policy provides a high level description of the arrangements in Stellar Healthcare for developing, implementing and monitoring IG policy and procedure. Detailed procedural guidance for staff is contained in separate specific documents listed in section 8 (below) and therefore, the contents of this document are most relevant to staff who exercise a supervisory or managerial role or have a role with an information management component.

3. Policy and Standards

Stellar Healthcare will ensure compliance with all relevant legislative requirements as well as with relevant Health and Social Care Information Centre (HSCIC) guidance and requirements. There will be an established and maintained policies and procedures aligned to the NHS Operating Framework.
As part of the organisation's obligation to ensure all staff are made aware of confidentiality requirements and procedures, a staff questionnaire has been developed for staff to complete and return to the Information Governance Lead. Please see Appendix 2

4. Roles and Responsibilities

4.1 Senior Information Risk Owner (SIRO)

The role of Senior Information Risk Owner (SIRO) has been assigned to the organisation Chief Executive (CE). The SIRO takes ownership of both organisations' information risks policy and acts as advocate for information risk to the Board.
The SIRO has ultimate responsibility for ensuring that the organisation corporately meets its legal responsibilities and for the adoption of internal and external governance requirements.
Specifically, the SIRO will ensure that –

- IG is explicitly referenced within both organisation's statement of internal controls
- Senior Information Risk Owner/s (SIROs) are identified and an Information Asset Owner designated for each separate database or other major information assets.
- Appropriate IG training is undertaken by all staff and those in key roles.
- The annual IG assessment via the Information Governance Toolkit is submitted by the 31 March each year and shared with the Care Quality Commission (CQC).
- The organisation achieves at least level 2 performance against all requirements identified in the IG Toolkit.
- Details of incidents including Serious Incident Requiring Investigation (SIRI) involving actual or potential loss of personal data or breach of confidentiality are reported through Risk and Reporting Systems.

4.2 Caldicott Guardian

The Caldicott Guardian is a member of the Board (with medical background) who has particular responsibilities for protecting the confidentiality of patients/service-user's information. Acting as the 'conscience' of the organisation, the Caldicott Guardian will actively support work to enable information sharing where it is appropriate to share, and will advise on options for lawful and ethical processing of information.
The Caldicott Guardian will also have strategic roles which involve representing and championing Information Governance requirements and issues at executive team level and where appropriate, at a range of levels within the organisation's overall governance framework.

4.3 Information Governance Lead

The Information Governance Lead will support the SIRO, Caldicott Guardian and Information Asset Owners (IAOs) in delivering assurance on the information governance agenda.
The IG Lead will provide overall lead and coordination of the information governance work programme and assurance framework.

4.4 Information Asset Owners (IAOs)

Designated Information Asset Owners (IAOs) are senior members of staff at director/assistant director level or heads of department responsible for providing assurance to the SIRO that information risks, within their respective areas of responsibility are identified and recorded and that controls are in place to mitigate those risks.

4.5 All Staff

The majority of staff handles information in one form or another. Staff who in the course of their work create, use or otherwise process information have a duty to keep up to date with, and adhere to, relevant legislation, case law and national guidance. The organisation's policies, procedures and guidance documents listed in section 8 (below) will reflect such guidance and compliance with these polices, and will ensure a high standard of information governance compliance.

All staff, whether permanent, temporary, contracted or contractors are responsible for ensuring that they are aware of their responsibilities in respect of Information Governance.

Breaches of confidentiality may be treated as serious disciplinary incidents which in some circumstances can lead to dismissal. All staff should ensure they are aware of the relevant policies and procedures in respect of any personal information they may process.

5. Openness

Stellar Healthcare the need for an appropriate balance between openness and confidentiality in the management and use of information.

Information will be defined and where appropriate kept confidential, underpinning the Caldicott principles and the regulations outlined in the Data Protection and Freedom of Information Acts.

Non-confidential information about the organisation and its services will be available to the public through a variety of means including the procedures established to meet requirements in the Freedom of Information Act 2000.
Under the Data Protection Act patients and staff may have access to their own personal information held by the organisation through the Subject Access Request (SARs) procedure. Please see Subject Access Request Policy for further guidance.

5.1 Information Governance Framework

Information will be defined and where appropriate kept confidential, underpinning the principles of Caldicott and the regulations outlined within the Data Protection Act 1998. Non-confidential information of the organisation and associated services will be made available to the public, in line with the requirements of the Freedom of Information Act 2000, via the organisation's publication scheme.

Patients will have access to information relating to their own health care, options for treatment available and their rights as patients to have choice. There will be clear procedures and arrangements for handling queries from patients and the public for staff to follow.

Stellar Healthcare will have clear procedures and arrangements for liaison with the press and broadcasting media.

Integrity of information will be developed, monitored and maintained to ensure that it is appropriate and fit for the purposes intended.

Availability of information for operational purposes will be maintained within set parameters relating to its importance via appropriate procedures and computer system resilience.

Stellar Healthcare regards all identifiable personal information relating to patients as confidential, compliance with legal and regulatory framework will be achieved, monitored and maintained.

Stellar Healthcare regards all identifiable personal information relating to staff as confidential except where national policy on accountability and openness requires otherwise.

Stellar Healthcare will establish and maintain policies and procedures to ensure compliance with the Data Protection Act 1998, Human Rights Act, Freedom of Information Act 2000 and the common law duty of confidentiality.

Awareness and understanding of all staff, with regards to their responsibilities, will be routinely assessed and appropriate training and awareness provided through staff induction and mandatory training sessions.

Risk assessment, in conjunction with overall priority planning of organisational activity will be undertaken to determine that the appropriate, effective and affordable information governance controls are in place.

5.2 Information Governance Management

Information Governance framework for Health and Social Care is formed by those elements of law and policy from which applicable information governance standards are derived, and the activities and roles which individually and collectively ensure that these standards are clearly defined and met. (Please see the organisation's IG Management Framework Policy for further details).

5.3 Confidentiality and Data Protection Assurance

Stellar Healthcare IG Staff Handbook, Confidentiality Code of Conduct and Data Protection Policy provide staff with clear guidance with regards to best practice and law.

Confidentiality of staff/service user information is of the utmost importance to the organisation and protocols for the sharing of information with third parties are in place to ensure compliance.

Stellar Healthcare Third Party Agreement will be put in place for all third parties (companies and individuals) who have access to their Personal Identifiable Data (PID).

5.4 Information Security Assurance

Stellar Healthcare will ensure there are appropriate policies and procedures in place to maintain effective and secure management of its information assets and resources.

Audits will be undertaken and commissioned to assess information and IT security arrangements on a regular basis.

The appointed Commissioning Support Unit (CSU) will continue to provide services on key information systems and information governance requirement will be built into the service specifications with them.

The appointed Commissioning Support Unit (CSU) as the provider of IT systems will ensure that there is an effective security on all IT systems, and assurance on the implementation of software countermeasures and management procedures in order protect the organisation's vital information assets against the effects of malicious software and other risks.

5.5 Clinical/Corporate Information Assurance

Responsibility for Information Quality and Records Management in the organisation has been assigned to Stellar Healthcare IG Lead. The post holder will ensure that policies and procedures are in place for all staff, and there are effective management and audits and commission of records. Wherever possible, information quality will be assured at the point of collection.

Stellar Healthcare will ensure their records/information are maintained to the highest quality in terms of its accuracy, timeliness and relevance.

Policies and procedures are in a place to ensure compliance with the Freedom of Information Act in accordance with the organisation's commitment to openness.

Policies and procedures are in place to ensure all corporate records are managed, stored and archived in line with governance standards and legislations.

Stellar Healthcare will promote effective records management through policies, procedures and training.

Stellar Healthcare will use "Records Management: NHS Code of Practice, Part 1 and Part 2" as its standard, for the management of all records.

5.6 Secondary Use Assurance

Stellar Healthcare will ensure that NHS standard definitions, values and validation programmes are incorporated within key systems.

Stellar Healthcare will ensure that, it monitors and improves data quality.

Stellar Healthcare will work with the Health and Social Care Information Centre (HSCIC) to fulfill its obligations, with regards to carrying out in relation to encouraging information sharing for purposes of research using new initiatives such as General Practice Extraction Service (GPES) and Calculating Quality Reporting System (CQRS). However patient confidentiality shall remain of paramount importance to the organisation.

Stellar Healthcare will use local and national benchmarking to identify possible data quality issues and analyse trends in information.

Stellar Healthcare will work with its main commissioning partners to assure itself of the validity of the organisation's data.

Stellar Healthcare will engage fully with the Audit Commission's Payment by Results (PbR) data assurance framework.

5.7 Information Sharing

The sharing of confidential patient-identifiable information should be governed by clear and transparent procedures that satisfy the requirements of law and guidance and regulate working practices in both the disclosing and receiving organisations. In some circumstances

these procedures and the underpinning standards should be set out within an agreed information sharing agreement (ISA) or protocol.

Stellar Healthcare may need to share confidential patient-identifiable information with a range of organisations. The purposes to be served by sharing information will either relate to the provision of care, including the quality assurance of that care, for the individual concerned or will be for non-care or secondary purposes e.g. service evaluation, patient complaints or care enquiries, research, finance, public health work etc.

Information sharing protocols can be a useful way of providing a transparent and level playing field for organisations that need to exchange information. They can provide assurance in respect of the standards that each party to an agreement will adopt. However, they do not in themselves provide a lawful basis for sharing confidential information. This can only be achieved from effectively informing patients about the possibility of sharing and the choices they have available to them, to limit sharing. If the patient says 'no' to sharing, then information may only be shared in exceptional circumstances. It is consent that determines whether information can be shared – with consent you don't need an information sharing agreement for sharing to be lawful, without consent an agreement is meaningless.

Information partners can be, but are not limited to:

- Other NHS Organisations
- Social Care and other Local Authority elements
- The Police
- Education Services
- Voluntary Sector Providers
- Private Sector Providers

Stellar Healthcare will identify its non-NHS information partners and begin a process to understand and document the information requirements of each partner.

Having identified all its non-NHS information partners and the business needs served by exchanging information, the organisation will develop a high-level protocol that sets out the basic information governance principles agreed with each organisation. This high level protocol will be augmented by specific sections which apply to each information-sharing partner, so that the organisation has appropriate information sharing protocols agreed with all of its main non-NHS information-sharing partners.

All information sharing protocols will be regularly reviewed and updated. The identification, documentation and protocols for sharing patient-identifiable information will be agreed with all new information-sharing partners, prior to any exchange of information taking place.

Please refer to the organisation's Information Sharing Protocol for specific guidance on the procedure for information sharing.

6. Training

Stellar Healthcare recognises the importance of an effective training structure and programme to deliver compliant awareness of IG and its integration into the day-to-day work and procedures.

All permanent/contract staff will complete the online mandatory training modules https://www.igtt.hscic.gov.uk/igte/index.cfm within first week of employment, with further training required for managers / team leaders, staff who process personal information, and staff with specific information roles. Training Needs Analysis (TNA) has been developed to for staff in key roles, as part of effective delivery of training programme.

7. Effective Safety Culture

Stellar Healthcare encourages and promotes an effective safety culture throughout the organisation.

An effective safety culture:

- Sees errors as learning opportunities
- Motivates individuals to talk and be 'open' about their own experiences by encouraging such experiences to be shared
- Responds to problems that are identified
- Does not unfairly 'penalise' those who have made errors
- Has a reporting system that is seen to uncover the underlying causes of incidents

Staff should feel at ease when reporting any incident/s that either do, or could potentially threaten information security. Examples of such incidents are as follows:-

- Using another user's login id/swipe card
- Unauthorised disclosure of information
- Leaving confidential / sensitive files out
- Theft or loss of IT equipment
- Theft or loss of computer media, i.e. floppy disc or memory stick
- Accessing a person's record inappropriately e.g. viewing your own health record or family members, neighbors, friends etc.,
- Writing passwords down and not locking them away
- Identifying that a fax has been sent to the wrong recipient
- Sending/receiving an sensitive email to/from "all staff" by mistake
- Giving out or overhearing personally identifiable information over the telephone
- Positioning of pc screens where information could be viewed by the public
- Software malfunction
- Inadequate disposal of confidential material (Placed into a general waste-bin)

Whilst the organisation is eager to avoid a 'blame culture' becoming embedded in any way, staff should be mindful that any staff member found to deliberately, recklessly or negligently breach confidentiality may be subject to disciplinary action, (including dismissal) face legal proceedings, or both dependent on the seriousness of the incident.

8. Dissemination and implementation

This policy will be publicised on the internet/intranet. Managers are required to ensure that their staff understand its application to their practice.

Awareness of any new content/change in process will be through the staff bulletin in the first instance. Where a substantive revision is made then a separate plan for communicating and implementing this change will be devised by the SIRO.

9. Related Documents from

The following documentation relates to the management of information and together underpins Stellar Healthcare Information Governance Assurance. This policy should be read in conjunction other policies:

- Information Governance Policy
- Confidentiality and Data Protection Policy
- Records Management Policy
- Incident Management and Reporting Procedures
- Information Security Policy
- Subject Access Request Policy
- Freedom of Information Policy
- Information Sharing Policy
- Safe Haven Policy
- Information Risk Policy
- Business Continuity Strategy

10. Equality, diversity and mental capacity

Stellar Healthcare recognises the diversity of the local community and those in its employment. The organisations aim to provide a safe environment free from discrimination and a place where all individuals are treated fairly, with dignity and appropriately to their need.

This policy was assessed against NHS Central Eastern Commissioning Support Unit Equality and Diversity assessment to ensure that it does not introduce any unexpected or unwarranted equality and diversity disparities.

Appendix 1 has been used to screen to this policy. The assessment confirmed that no amendments are required at this time.

Glossary Term	Definition
CSU	Commissioning Support Unit
CQRS	Calculating Quality Reporting System
IG	Information Governance
FOIA	Freedom of Information Act
DPA	Data Protection Act
GPES	General Practice Extraction Service
IGT	Information Governance Toolkit
IGTT	Information Governance Training Tool
ISA or ISP	Information Sharing Agreement or Protocol
SIRO	Senior Information Risk Owner

Appendix 1: Equality Analysis

1	Does the policy/guidance affect one group less or more favorably than another on the basis of:	Yes/No	Comments
	Race	No	
	Ethnic origins (including gypsies and travellers	No	
	Nationality	No	
	Gender	No	
	Culture	No	
	Religion or belief	No	
	Sexual orientation including lesbian, gay and bisexual people	No	
	Age	No	
	Disability (e.g. physical, sensory or learning	No	
	Mental health	No	
2	Is there any evidence that some groups are affected differently?	No	
3	If you have identified potential discrimination, are any exceptions valid, legal and/or justifiable	No	
4	Is the impact of the policy/guidance likely to be negative	No	
5	If so can the impact be avoided?	N/A	
6	What alternatives are there to achieving the policy/guidance without the impact?	N/A	

Appendix 2: Confidentiality Awareness Questionnaire

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

Part of this obligation is to ensure that all staff are trained and made aware of confidentiality requirements and procedures. As a result the organisation would like to ask staff to complete this quick questionnaire so it can establish if the current procedures in place are adequate and effective enough to raise awareness and maintain compliance with confidentiality requirements.
Please return to the IG Lead when completed for your department.

1) Please state the department you work for: _____

2) Have you received any of the following training regarding confidentiality whilst working in the organisation;

a. Induction Training? _____

b. Information Security and Confidentiality training / Information Governance Training? _____

3) Can you provide an approximate date of your most recent confidentiality based training or information received? (**this may be a leaflet or poster**)

_____

4) If you have any concerns or issues regarding confidentiality to whom would you turn to for advice?

_____
_____

5) What would you do if you suspect a possible breach of confidentiality?

_____
_____

6) If a patient's or staff's record goes missing, are you aware of the procedures / policy to follow (please specify if known)?

_____
_____

7) Can you name any of the policies that the organisation follows on confidentiality?

_____
_____
_____

8) Where would you find them?

_____
_____

9) Name one of the main acts of parliament that has confidentiality as its central focus?

_____

10) Who is you Department's Information Asset Owner?

_____

11) Can you name your Caldicott Guardian? _____

12) Can you name your Senior Information Risk Owner? _____

13) If a Patient or staff requests a copy of the information you hold:
Who would you inform? _____
Do you have to release the records? _____
How long do you have to respond? _____

Any other comments in reference to confidentiality you may have:
_____
_____