North Staffordshire Combined Healthcare NHS Trust

Document level: _____
Code: 7.21
Issue number: _____

Information Risk Security Policy

Lead executive	Director of Finance
Authors details	Information Security Manager

Type of document	Policy
Target audience	All Staff
Document purpose	Information

Approving meeting	FPD Trust Board	Meeting date	7th February 2019 28th February 2019
Implementation date	28th February 2019	Review date	28th February 2022

Trust documents to be read in conjunction with	
4,18a & b	Risk Management Policy and Strategy
7.03	Information Security and Data Protection Policy
7.19	Mobile Information Handling Policy
7.14	Safe Haven Policy
7.16	IT Asset Management Policy
5.01	Incident Reporting Policy

Document change history		Version	Date
What is different?	Policy has been revised due to legislation changes to Data Protection and updates in Trust Information Protection procedures		
Appendices / electronic forms	As previous		
What is the impact of change?	Updating due to change in legislation. Advising of changes to SIRO and Caldicott Guardian training as the IG Training Tool additional modules were withdrawn in 2017 and have not been replaced, therefore it is for the Trust to arrange external training for relevant members of staff.		

Training requirements	In addition to the mandated annual Data Protection Awareness training module all staff are required to complete, the Trust also needs to arrange additional learning for relevant staff via an external consultant.

Document consultation	
Directorates	
Corporate services	
External agencies	

Financial resource implications	Cost of external trainer/contractor for one day.

External references
1. Data Protection Act 2018 2. General Data Protection Regulation (GDPR)

Monitoring compliance with the processes outlined within this document	This policy will be monitored and updated by the Information Governance Steering Group.

Equality Impact Assessment (EIA) - Initial assessment	**Yes/No**	**Less favourable / More favourable / Mixed impact**
Does this document affect one or more group(s) less or more favorably than another (see list)?		
– **Age** (e.g. consider impact on younger people/ older people)	No	
– **Disability** (remember to consider physical, mental and sensory impairments)	No	
– **Sex/Gender** (any particular M/F gender impact; also consider impact on those responsible for childcare)	No	
– **Gender identity and gender reassignment** (i.e. impact on people who identify as trans, non-binary or gender fluid)	No	
– **Race / ethnicity / ethnic communities / cultural groups** (include those with foreign language needs, including European countries, Roma/travelling communities)	No	
– **Pregnancy and maternity, including adoption** (i.e. impact during pregnancy and the 12 months after; including for both heterosexual and same sex couples)	No	
– **Sexual Orientation** (impact on people who identify as lesbian, gay or bi – whether stated as 'out' or not)	No	
– **Marriage and/or Civil Partnership** (including	No	

heterosexual and same sex marriage) – **Religion and/or Belief** (includes those with religion and /or belief and those with none) – **Other equality groups?** (may include groups like those living in poverty, sex workers, asylum seekers, people with substance misuse issues, prison and (ex) offending population, Roma/travelling communities, and any other groups who may be disadvantaged in some way, who may or may not be part of the groups above equality groups)	No No	
If you answered yes to any of the above, please provide details below, including evidence supporting differential experience or impact.		
Enter details here if applicable		
If you have identified potential negative impact: - Can this impact be avoided? - What alternatives are there to achieving the document without the impact? Can the impact be reduced by taking different action?		
Enter details here if applicable		
Do any differences identified above amount to discrimination and the potential for adverse impact in this policy?	Yes / No	
If YES could it still be justifiable e.g. on grounds of promoting equality of opportunity for one group? Or any other reason	Yes / No	
Enter details here if applicable		
Where an adverse, negative or potentially discriminatory impact on one or more equality groups has been identified above, a full EIA should be undertaken. Please refer this to the Diversity and Inclusion Lead, together with any suggestions as to the action required to avoid or reduce this impact. For advice in relation to any aspect of completing the EIA assessment, please contact the Diversity and Inclusion Lead at Diversity@northstaffs.nhs.uk		
Was a full impact assessment required?	No	
What is the level of impact?	Low	

CONTENTS

Glossary

DPO	Data Protection Officer
IAAF	Information Asset Audit Form (*Appendix A)*
IAA	Information Asset Administrator
IAO	Information Asset Owner
IG	Information Governance
IGM	Information Governance Manager
ISM	Information Security Manager
SIRO	Senior Information Risk Owner

1. Policy Statement

Information risk is inherent in all administrative and business activities and everyone working for or on behalf of the Trust continuously manages information risk. This policy recognises that the aim of information risk management is not to eliminate risk, but rather to provide the structural means to identify prioritise and manage the risks involved in all Trust activities. It requires a balance between the cost of managing and treating information risks with the anticipated benefits that will be derived from using information appropriately.

Information risk management is an essential element of broader information governance and is an integral part of good management practice. The intent is to embed information risk management in a very practical way into business processes and functions.

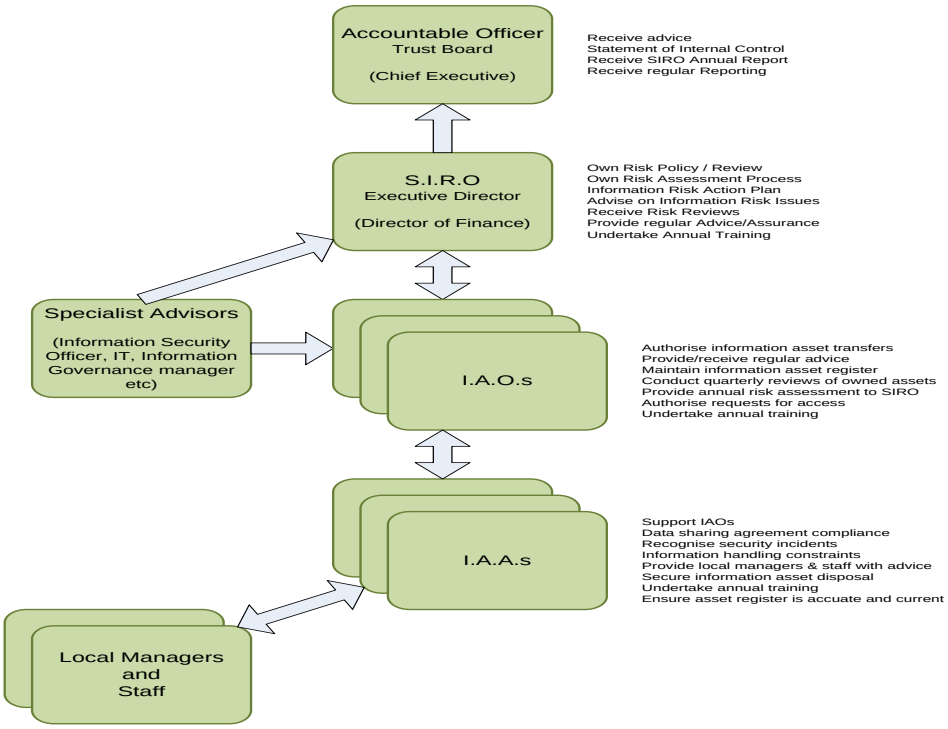
It should be noted that this policy complements and does not supersede the Trusts Risk Management Policy and Strategy documents.

2. Scope

This policy applies to all areas of the Trust and all individuals employed by the Trust, including contractors, voluntary workers, students, locum and agency staff.

When an Information Asset is identified Information Asset Audit Forms (IAAF) will be completed *(see Appendix A)* containing a standard Trust Risk Assessment. This will be reviewed and, where necessary, updated annually. If any risks are escalated to a "high" rating; they should be reported and entered on the Trusts Risk Register. Risk Assessments should be completed in line with the Trusts Risk Management Policy and reviewed at regular intervals.

3. Duties



3.1 Chief Executive

The Chief Executive as the Accountable Officer for the Trust has overall accountability and responsibility for Data Security Protection in the Trust and is required to provide assurance through the Statement of Internal Control that all risks to the Trust, including those relating to information, are effectively managed and mitigated. Details of Serious Untoward Incidents involving data loss or confidentiality breach must also be reported in the annual report.

3.2 Senior Information Risk Officer

The Director of Finance is responsible to the Chief Executive for IG and is the designated Senior Information Risk Owner (SIRO), who takes ownership of the Trust's Information Risk Policy, acts as advocate for information risk on the Board and provides written advice to the Accountable Officer on the content of the Statement of Internal Control in regard to information risk.

3.3 Caldicott Guardian

The Caldicott Guardian is the "conscience" of the organisation, providing a focal point for patient confidentiality and information sharing issues, and advising on the options for lawful and ethical processing of information as required. The Caldicott Guardian and SIRO are both concerned with ensuring NHS data is protected and is not stored, accessed or used inappropriately. The SIRO and any organisational IAOs work closely with the Caldicott Guardian and consult him/her where appropriate when conducting information risk reviews for assets which comprise or contain patient information. In most NHS Trusts the Caldicott Guardian is the Medical Director.

3.4 Data Protection Officer

The Data Protection Officer interprets national guidance and legislation to develop policy, strategy and systems to ensure compliance with Information Governance Data Protection requirements and the achievement of data quality standards in line with the GDPR, providing leadership, challenge and support to achieve organisational compliance.

3.5 Information Security Manager

The Information Security Manager (ISM) will be responsible to the SIRO and IAOs for the identification, delivery and management of an information risk management programme to address and manage risks to the Trusts Information Assets.

3.6 Information Asset Owners

Appropriate staff will be designated Information Asset Owners (IAOs) with responsibility for the completion and maintenance of the Trust's Information Asset Register; for providing assurance to the SIRO that information risks within their respective directorate have been identified and recorded, and that controls are in place to mitigate those risks. The Information Asset Audit Forms (see Appendix A) will be completed/reviewed on an annual basis, for each asset, and forwarded to the ISM each year. This information will be collated to provide evidence for the Data Security Protection Toolkit.

3.7 Information Asset Administrators

IAOs can appoint Information Asset Administrators (IAAs) to support them in the delivery of their information risk management responsibilities for the Directorate. IAAs ensure that policies and procedures are followed, recognise actual or potential security incidents and take steps to mitigate those risks, consult their IAO on incident management, and ensure that information asset registers are accurate and up to date.

3.8 Chief Information Officer

The CIO is responsible for managing the information Governance agenda across the Trust. This will include monitoring compliance with those requirements around Information Risk Management within the Data Security Protection and ensuring these standards are met.

3.9 All Staff

Everyone has a role in the effective management of information risk. All staff will actively participate in identifying potential information risks in their area and contribute to the implementation of appropriate treatment actions. All Trust staff and anyone else working for CHT (e.g. agency staff, honorary contracts, management consultants etc.) who use and have access to Trust information must understand their personal responsibilities for information governance and comply with the law. All staff must comply with Trust policies, protocols, procedures and guidance and attend relevant education and training events.

4. Framework

4.1 Policy objectives

The Information Risk Policy has been created to:

- Protect the Trust, its staff and its patients from information risks where the likelihood of occurrence and the consequences are significant;
- Provide a consistent risk management framework in which information risks will be identified, considered and addressed in key approval, review and control processes;
- Provide assistance to and improve the quality of decision making throughout the Trust;
- Meet legal or statutory requirements and assist in safeguarding the Trust's information assets.

4.2 Information Security

The aim of Information Security is to establish and maintain the security and confidentiality of information, information systems, applications and networks owned or held by the Trust.

North Staffordshire Combined Healthcare is committed to achieving the following Information Security and IG objectives:

- The Trust will establish and maintain policies for the effective and secure management of its information assets and resources
- The Trust will undertake or commission annual assessments and audits of its information and IT security arrangements
- The Trust will promote effective confidentiality and security practice to its staff through policies, procedures and training
- The Trust will establish and maintain incident reporting procedures and will monitor and investigate all reported instance of actual or potential breaches of information confidentiality and security.

4.3 Information Assets

The guidance contained within this policy and its related materials applies to NHS information assets of all types. These information assets may consist of:

- Digital or hard copy patient health records (including those concerning all specialties and GP medical records);
- Digital or hard copy administrative information (including, for example, personnel, estates, corporate planning, supplies ordering, financial and accounting records);

Digital or printed X-rays, photographs, slides and imaging reports, outputs and images;

- Digital media (including, for example, data tapes, CD-ROMs, DVDs, USB disc drives, removable memory sticks, mobile phones and other internal and external media compatible with NHS information systems);
- Computerised records, including those that are processed in networked, mobile or standalone systems;
- Email, text and other message types such as Goldfax (eFax solution)

4.4 Training

The HSCIC - Data Security Protection Training Tool is an online training tool focused on all aspects of learning about Data Security Protection .The aim of the tool is to develop and improve staff knowledge and skills in the IG work area. Annual training on this system is mandatory for all staff.

The Trust's Information Risk Management programme will require the Caldicott Guardian, SIRO, IAO's and IAA's to complete additional training relevant to their responsibility.

4.5 Key definitions are:

- **Risk**
  The chance of something happening which will have an impact upon objectives. It is measured in terms of consequence and likelihood.
- **Consequence**
  The outcome of an event or situation, expressed qualitatively or quantitatively, being a loss, injury, disadvantage or gain.
- **Likelihood**
  A qualitative description or synonym for probability or frequency.
- **Risk Assessment**
  The overall process of risk analysis and risk evaluation.
- **Risk Management**
  The culture, processes and structures that are directed towards the effective management of potential opportunities and adverse effects.
- **Risk Treatment**
  Selection and implementation of appropriate options for dealing with risk. Conceptually, treatment options will involve one or a combination of the following five strategies:
    - Avoid the risk
    - Reduce the likelihood of occurrence
    - Reduce the consequences of occurrence
    - Transfer the risk
    - Retain/accept the risk
- **Risk Management Process**

  The systematic application of management policies, procedures and practices to the task of establishing the context, identifying, and analysing, evaluating, treating, monitoring and communicating risk.

5. Implementation and Monitoring

The Information Risk Management process will be reviewed annually against the HSCIC Data Security Protection Toolkit to identify key areas for continuous improvement.

The Data Security Protection Toolkit contains guidance on expected standards and key performance indicators, which together will be used to monitor the effectiveness of this policy and the Information Risk Management programme. Reports will be generated to monitor the training within the Data Security Protection Toolkit.

6. Associated Policy and Procedural Documentation

6.1 Related policies/guidelines – Local

This document should be read in addition to the following policies found on the Trust Intranet website (SID)

Risk Management Policy and Strategy

Information Security & Data Protection Policy

Mobile Information Handling Policy

Safe Haven Policy

Incident Reporting Policy

IT Asset Management Policy

Data Quality Policy

Information Governance Assurance Framework

6.2 Related policies/guidelines – National

Department of Health Information Security Management NHS Code of Practice – April 2007

NHS Information Risk Management Digital Information Policy – January 2009

Data Protection Act 2018

General Data Protection Regulation (GDPR)

DoH Records Management Code of Practice

7. Incident Reporting

The reporting of Serious Incidents (including Cyber Incidents) relating to potential or actual breaches of confidentiality involving person identifiable data, including data loss, will be in line with the Trusts overall incident reporting processes, following the procedure outlined in the Trusts Incident Reporting Policy, and via the Data Security Protection Toolkit for any incidents hitting Level 2 or above.

Training Needs Analysis for the policy for the development and management of Trustwide procedural / approved documents
Please tick as appropriate

There **is no** specific training requirements- awareness for relevant staff required, disseminated via appropriate channels (Do not continue to complete this form-no formal training needs analysis required)	✓
There **is** specific training requirements for staff groups (Please complete the remainder of the form-formal training needs analysis required-link with learning and development department.	

Staff Group	✓ if appropriate	Frequency	Suggested Delivery Method (traditional/ face to face / e-learning/handout)	Is this included in Trustwide learning programme for this staff group (✓ if yes)
Career Grade Doctor				
Training Grade Doctor				
Locum medical staff				
Inpatient Registered Nurse				
Inpatient Non-registered Nurse				
Community Registered Nurse				
Community Non Registered Nurse / Care Assistant				
Psychologist / Pharmacist				
Therapist				
Clinical bank staff regular worker				
Clinical bank staff infrequent worker				
Non-clinical patient contact				
Non-clinical non patient contact				

Please give any additional information impacting on identified staff group training needs (if applicable)

Please give the source that has informed the training requirement outlined within the policy i.e. National Confidential Inquiry/NICE guidance etc.

Any other additional information

Completed by		Date	