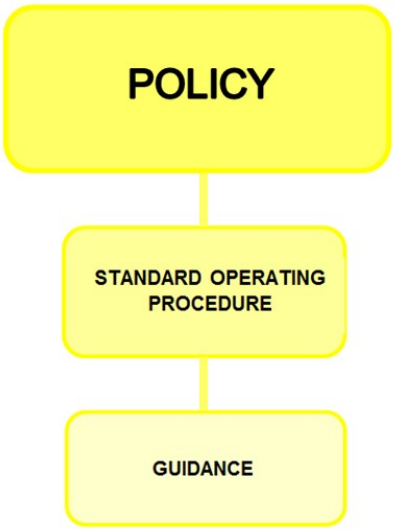
Lancashire Care NHS
NHS Foundation Trust

INFORMATION GOVERNANCE POLICY

UNIQUE POLICY REFERENCE	IM&T 011
APPROVAL DATE	28th March 2017
REVIEW DATE	November 2018
POLICY AUTHOR	Information Governance, Assurance and Compliance Lead
ACCOUNTABLE DIRECTOR	SIRO/Director of Finance
APPROVED BY	Deputy SIRO

TRUST GOVERNANCE STRUCTURE
POLICY LINKED TO *Corporate Governance & Compliance Sub-Committee*



POLICY VERSION CONTROL

This record shall detail all previous versions of the Policy, including versions that have been known by other names and the date of when a new version was created.

Previous Versions (Title)	Date Reviewed	Why was a new version created?
Information Governance Policy	Sept 2015	Policy updated in new Trust Corporate Policy format and includes reference to new IAO/IAA structure

1. TRUST POLICY STATEMENT

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

It is of paramount importance to ensure that information is efficiently managed and that our policies, procedures, management accountability and structures provide a robust governance framework for the continual improvement of information management.

The Trust will establish and maintain policies and procedures to ensure compliance with the principles of the Data Protection Act 1998 (DPA) including when appropriate the *General Data Protection Regulations (GDPR)* and associated legislation and regulation including:

- The Privacy and Electronic Communications Regulations (PECR) 2016
- The Computer Misuse Act 1990
- The Freedom of Information Act 2000
- Health and Social Care Act 2012

The aim of this policy is to provide the employees of Lancashire Care NHS Foundation Trust with a framework through which compliance with Information Governance (IG) legislation will be met.

Compliance will also be met through National context such as:

- NHS Digital Information Governance Toolkit (IGT)
- Professional codes of conduct from the BMA, GMC and NMC and others including Allied Health professionals, Finance Professionals, Psychological Professionals and NHS Managers
- Confidentiality NHS Code of Practice
- The 'Information Security Management: NHS Code of Practice
- NHS Care Record Guarantee
- Records Management Code of Practice for Health and Social Care 2016

2. APPLICATION

This policy applies to all staff working within the Trust, including any individual directly employed or indirectly employed by the organisation, for example: third party contracting staff, students, temporary staff, volunteers, locum or bank staff and any individual who has been given access to Trust network or systems.

.

Managers within the Trust are responsible for ensuring that the policy and its supporting standards and guidelines are built into local processes and that there is ongoing compliance with policy.

This policy applies to the governance of information, produced, processed, handled, used, shared and transferred by the Trust including any form of

- Patient information
- Human resources information
- Finance information
- Governance information
- Organisational administrative information

This Policy covers:

- All information used by the organisation;
- All information systems managed by or used by the organisation;
- Any individual using information "owned" by the organisation;
- Any individual requiring access to information "owned" by the organisation.

3. IMPLEMENTATION

In order to comply with the Policy, staff must ensure that they familiarise themselves with relevant policies and guidance and that they understand the responsibilities set out in them. If individuals are unsure about any aspect of a Policy or guidance they must seek clarification from their line manager or the Information Governance (IG) team. Staff must ensure that they are compliant with legislative and regulatory requirements on a day to day basis.

All Managers are responsible for ensuring that the Policy and its supporting standards and guidance are built into local processes and that there is on-going compliance on a day to day basis with regards to confidentiality and information sharing. Further details of these standards can be found in the IG SOP.

It is the role of the Executive Director, Senior Information Risk Owner (SIRO), Caldicott Guardian or authorised designate, to ratify Trust Corporate policies in respect of Information Governance, taking into account legal and NHS requirements. The Board is also responsible for ensuring that sufficient resource is provided to support the requirements of this policy.

This Policy works in conjunction with other related Policies and Procedures e.g.

- Information Governance Procedure
- Data Quality Policy
- IM&T Security Policy and Procedure
- Procedure for Communicating via E-mail, Text (SMS) and Video Communications
- Access to Health Records Policy
- Policy for Health Records Management
- Health Records Security and Confidentiality Policy
- Policy for the use of Mobile Communication Devices
- Registration Authority Policy (RA)
- Freedom of Information Policy
- Corporate Records Management Policy and Procedure
- Sharing and Disclosure of Information with External Agencies

Information Governance related policies can be found at

http://trustnet/docs/policies/DOCUMENTS%20POLICIES/Forms/corporate.aspx

Any breach or suspected breach of confidentiality or information security, including cyber security events, must be reported to a senior manager, recorded on Datix and where identified as serious referred for immediate investigation. A breach of this policy could lead to action from the Information Commissioners Office which may include a monetary penalty of up to £500,000.

The Trust will ensure that information will be provided to the public where required by law. Subject Access Requests will be dealt with in line with the Access to Health Records Policy and Freedom of Information Requests will be process in line with the Freedom of Information Policy.

4. COMPLIANCE

The IG Lead will ensure that there is a robust IG Framework in place across the Trust. Full details of the IG Framework can be found in the IG Standard Operating Procedure.

The formal Information Asset Owner and Administrator (IAO / IAA) governance structure must support compliance with all Trust Policies, procedures and practices**.** Senior IAO's will be expected to provide regular reports to the SIRO to provide assurance of Network IG compliance with this Policy.

Information Governance must be part of Network and Support Services Governance agenda to ensure that risks to compliance are reviewed and discussed and operational actions put in place to address the management of those risks. Reports from these meetings will form part of senior management reporting to both the Chief Operating Officer and the SIRO.

Information Governance training is mandatory for all staff directly employed or otherwise by the organisation for example, third party contracting staff, students, temporary staff, volunteers, locum or bank staff and any individual who has been given access to Trust network or systems and is part of the Trust Mandatory Training Policy. Completion of Mandatory IG training is monitored to ensure compliance with the Information Governance Toolkit (IGT Requirement 112) standard requiring 95% of the required staff mentioned earlier working for the Trust to have completed the annual Mandatory training module.

Monitoring of IG Compliance and assurance is also evidenced as part of the Information Governance Toolkit annual submission. The IG team will work with IAO/IAA's to co-ordinate evidence required to achieve level two for all requirements (minimum of 65%) and attain a 'satisfactory' rating. An audit is also undertaken by the Trust Internal auditors on an annual basis to assess the validity and governance of the annual IGT submission.

5. COMMUNICATION

The Policy will be made available in a variety of ways as outlined in the Policy Communications Plan. In the first instance a new Policy will be advised via the Trust Weekly bulletin. A second delivery method will be employed to deliver the Policy direct to user's desktop so that the Trust has

confirmation of receipt. The Policy will be accompanied by a short survey to verify the users understanding of the Policy.

All managers are responsible for ensuring that new starters and current staff have access to Trust Policy and Procedures as appropriate e.g. either electronically or in paper form dependent on the staff working arrangements and environment.

Additional Policy training and awareness can be provided on request where a specific need is identified to the IG team.

6. MONITORING INTEGRITY OF THE SYSTEM

The IG Lead is responsible for keeping up to date with changes to legislation and regulation and reflecting those changes in Policy and procedures where they have an impact on compliance and practice across the organisation. Any significant change to the Policy will be subject to peer review prior to appraisal and ratification by the SIRO. The Policy will be issued as a new version and made available as per the methods identified in the Policy Communications Plan.