

Information Governance Management Policy

(Smartcard & ID Cards, Freedom of Information and EIR)

Reference No:	P_IG_25
Version:	2
Ratified by:	LCHS Trust Board
Date ratified:	14 August 2018
Name of originator/author:	Kaz Scott, Information Governance Lead
Name of responsible committee/individual:	Information Governance Management Assurance Group
Date issued:	November 2018
Review date:	August 2020
Target audience:	All staff & Third Party Contractors employed by LCHS
Distributed via:	Website

Lincolnshire Community Health Services NHS Trust

Information Governance Management Policy

Version Control Sheet

Version	Section/Para/ Appendix	Version/Description of Amendments	Date	Author/ Amended by
1	All	Amalgamation of policies P_IG_01, 06, 08, 18 content previously ratified and further content update to reflect GDPR. Fully Reviewed.	June 2018	Kaz Scott
2	2	Updated Smartcard Terms and Conditions	November 2018	Kaz Scott
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				

Copyright © 2018 Lincolnshire Community Health Services NHS Trust, All Rights Reserved. Not to be reproduced in whole or in part without the permission of the copyright owner.

Lincolnshire Community Health Services NHS Trust

Information Governance Management Policy

Contents

i) Version Control Sheet	Page
ii) Policy Statement	4
Information Governance Management	5 - 10
Smartcard and Identity Cards	11 - 16
Freedom of Information and EIR	17 - 22
NHSLA Monitoring	23
Equality Analysis	24

Lincolnshire Community Health Services NHS Trust

Information Governance Management Policy

Policy Statement

Background Information Governance Management (IGM) ensures the Trust has a robust and documented framework for managing Information Governance (IG) that extends throughout the Trust.

This must be used in conjunction with other policies and guidance produced by the Trust.

Statement

IGM is to provide clear and effective management and accountability structures, governance processes, documented policies and procedures, a comprehensive IG training programme and adequate resources to manage and embed IG throughout the Trust.

It pulls together all of the requirements to ensure that personal information is processed legally, securely, efficiently and effectively in order to deliver the best possible care to patients.

This runs in parallel with Clinical Governance, Research Governance and Corporate Governance.

The policy is split into sections and details specific procedures for achievement of the policy standards.

Responsibilities This policy applies to:

- All staff including Temporary, Contractors and sub-Contractors
- All information and systems used or managed by the Trust
- Any individual using information or requiring access 'owned' by the Trust

Training All staff, including temporary staff and Third Party Contractors working on behalf of the Trust will have access to IG Training through Mandatory, Induction or IAO/IAA which may also be delivered by e-learning.

Dissemination The policy will be published on the Trust website.

Resource implication Resource implications are primarily in relation to staff awareness and additional training to ensure compliance with agreed standards.

INFORMATION GOVERNANCE MANAGEMENT

Information plays a key part in the clinical and corporate governance and the quality in the provision of patient services, planning, performance measurement, assurance and financial management relies upon accurate and available information.

IG is supported under a Service Level Agreement (SLA) for the provision of services which consists of: Registration Authority (RA), Freedom of Information and Information Communication Technology (ICT).

The Information Governance Assurance Framework (IGAF) is the national framework of standards that brings together all statutory, mandatory and best practice requirements concerning information management. The standards are set out in the Data Security and Protection Toolkit (DSPT) as a road map enabling organisations to plan and implement standards of best practice and to measure and report compliance on an annual basis.

IG provides a framework for the Trust to be assured that information processes are appropriately secure and legal. This relies on good quality information being available at the point of need in order to provide a quality service. Staff need to have confidence in the quality of data they use to make decisions about patient care and treatment and the way in which we use resources and run the business.

Robust IG requires clear and effective management and accountability structures, governance processes, documented policies and procedures, trained staff and adequate resources.

It brings together all of the requirements, standards and best practice that apply to the processing of personal information to ensure:

- Compliance with the law
- Implementation of DH Guidelines
- Planned year on year improvement
- DSPT Requirements

Objectives of IG

- Information will be organised and managed in accordance with mandated and statutory standards and kept confidential where appropriate.
- The integrity of information is assured, monitored and maintained, to ensure that it is of quality and reliable for use for the purposes that it is collected and used for.
- Information required for operational purposes is kept secure and available to and accessed by those who need it.
- Compliance with legal and regulatory frameworks is achieved, monitored and maintained.
- All staff will have access to appropriate training and education to ensure they understand their responsibilities for managing information
- An information risk management strategy is implemented to ensure ownership of and accountability for the Trust's information assets and the mitigation of associated risks.

Operating Frameworks

The IG element of the Operating Framework includes the requirement for the effective use of NHS numbers, the Summary Care Record Portal (SCR) and the National Back Office (NBO) to support data quality and the efficient and appropriate sharing of patient information with partners in the delivery of patient care. It also includes the requirement for all NHS organisations to achieve compliance against all key assertions in the DSPT.

The Trust is responsible for ensuring that all organisations which we share data with; including independent contractors and the third sector, achieve the IGAF requirements.

Information security and confidentiality must remain a key priority in ensuring continued delivery of a quality health and patient centred health service. It is imperative that the Trust ensures that the robust arrangements that have been developed with regard to IG are not compromised in the light of any organisational change and that accountabilities remain clear.

Data Security and Protection Toolkit (DSPT)

The annual information governance assessment is measured via a self-assessment process of compliance against the assertions set out in the DSPT and verified by Internal Audit Review. The DSPT is based on the National Data Guardian 10 Data Security Standards;

NHS organisations are required to submit online IG performance reports to NHSD, which can be tracked by Commissioners and other monitoring bodies. There are 2 submissions:

- 31st October – Performance
- 31st March - Final Self-Assessment Report

The final performance assessment is submitted to NHSD each year and shared with the Care Quality Commission (CQC) and the Audit Commission and are available to the general public.

IG Training and Development

IG Training and Development is essential for the development and improvement of staff knowledge and skills relating to IG. IG training must extend beyond basic confidentiality and security awareness in order to develop and follow best practice.

Staff need to understand the value of information and their responsibility for it, which includes data quality, information security, records management, confidentiality, legal duty, information law and rights of access and patient's rights in terms of a right of privacy and choice.

The Trust, supported by the SIRO, the IG Lead and Education and Workforce Development Team (EWDT) are responsible for the development and delivery of IG Training, supported in its implementation by IGMAG.

The Trust utilises the following training methods:-

- The Electronic Staff Record (ESR) to book staff onto Induction for New Starters or Block Annual Mandatory Training delivered to staff.
- E-Learning for IAO/IAA to support the Trust Information Asset Register.
- Bespoke IG training sessions are also provided as and when required.
- Security alerts/guidance is published on a regular basis.

IG brings together the requirements and standards for handling patient, staff and corporate information including:

- All staff ensure that all Personal Confidential Data (PCD) is handled, stored and transmitted securely. PCD is only shared for lawful and appropriate purposes.
- All staff understand their responsibilities under the National Data Guardian's (NDG) Data Security Standards, including their personal accountability for deliberate or avoidable breaches.
- All staff complete appropriate annual data security training and pass a mandatory test.

- PCD is only accessible to staff who need it for their current role. All access to PCD on IT systems can be attributed to individuals.
- Processes are reviewed at least annually to identify and improve processes which have caused breaches or near misses.
- 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.
- 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.
- No unsupported operating systems, software or internet browsers are used within the IT estate.
- 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.
- Suppliers are held accountable via contracts for protecting the personal confidential data they process and meeting the NDG Data Security Standard.

Additional Information Governance Training by Staff Role

Job Role	Mandatory Modules as determined by the Trust	Timeframe
Caldicott Guardian	<ul style="list-style-type: none"> • Caldicott Guardian • Data Security Awareness Level 1 	Annual
Data Protection Officer	<ul style="list-style-type: none"> • Data Protection • Risk Management • Data Security Awareness Level 1 	Annual
Information Governance and Support Staff	<ul style="list-style-type: none"> • Caldicott Guardian • Risk Management • Data Security Awareness Level 1 	Annual
Senior Information Risk Owner (SIRO)	<ul style="list-style-type: none"> • Risk Management • Data Security Awareness Level 1 	Annual
Information Asset Owner or Administrator (IAO / IAA)	<ul style="list-style-type: none"> • Data Security Awareness Level 1 	Annual
Head of IMT and IMT Support Staff	<ul style="list-style-type: none"> • Data Security Awareness Level 1 	Annual
Records Management - Subject Access / Child Health Staff	<ul style="list-style-type: none"> • Data Security Awareness Level 1 	Annual
Information Analysts, Clinical Coders	<ul style="list-style-type: none"> • Data Security Awareness level 1 	Annual
System Sponsors / Card Administrators	<ul style="list-style-type: none"> • CIS E-learning recommended 	1 hour

Risk Assessment and Management Process

Potential losses arising from breaches of IT and information security include physical destruction or damage to the organisation's computer systems, loss of system availability and the theft, disclosure or modification of information due to intentional or accidental unauthorised actions. In addition, healthcare organisations process Personal Confidential Data (PCD) of particular sensitivity, which needs to be protected from loss or inappropriate disclosure.

Incident Management

Guidance on incident management can be found under the Risk Management section of the Trust Policies.

Key Responsibilities and IG Accountability

Board of Directors

The NHS Chief Executive has made it clear that ultimate responsibility for IG in the NHS rests with the Board of each organisation, who should note that:

Details of serious incidents involving actual or potential loss of personal data or breach of confidentiality must be published in annual reports and reported through the IG Incident Reporting Tool which is available to the Information Commissioner (where necessary).

Chief Executive

The Accounting Officer (AO) is the Chief Executive who has overall responsibility for ensuring that information risks are assessed and mitigated to an acceptable level. Information risks are handled in a similar manner to other risks such as financial, legal and reputational risks.

Reference to the management of information risk and associated information governance practice is now required in the Statement of Internal Control which the AO is required to sign annually.

Senior Roles within the Trust supporting the IG agenda are held by the Caldicott Guardian (CG), Data Protection Officer (DPO), Senior Information Risk Owner (SIRO), Information Governance Lead (IGL) and some Commissioning Support provision under an SLA.

The CG role:-

- Is advisory
- Is the conscience of the organisation
- Provides a focal point for patient confidentiality and information sharing issues
- Is concerned with the management of patient information

The CG is the person with overall responsibility for protecting the confidentiality of PCD. The CG plays a key role in ensuring the Trust and partner organisations abide by the highest level of standards for handling PCD.

They are responsible for ensuring the Trust adheres to the Caldicott Principles. It is the responsibility of the CG to feedback any IG issues to the appropriate senior management board.

The SIRO role:-

- Is accountable
- Fosters a culture for protecting and using data
- Provides a focal point for managing information risks and incidents
- Is concerned with the management of all information assets.

The SIRO is an executive Board member with allocated lead responsibility for the Trust's information risks and provides a focus for the management of information risk at Board level.

The DPO

- Monitors the Trust compliance on the General Data Protection Reregulation 2016 and Data Protection Act 2018 using the DSPT
- Provides advice to the Trust on matters of data protection where required
- Co-operates with the supervisory authority
- Act as the central point with regards the supervisory authority

IG

IG in conjunction with the DPO are accountable for ensuring effective management, accountability, compliance and assurance for all aspects of IG. The key tasks include:

- Responsibility for delivering a high quality specialist IG service to the Trust
- To provide strategic direction, planning and guidance to ensure compliance with IG legislation and the national agenda
- Ensure work practices are evaluated and supported through the development of appropriate policy and procedures across the Trust

Information Governance Management Assurance Group (IGMAG),

With appropriate authority, has responsibility for the IG Agenda and works alongside the Countywide Information Governance Management Group (CWIMG) and the Quality and Risk Committee (Q&R). IGMAG will sign off all elements of the IG Agenda on behalf of the Trust.

The senior level of management receives periodic assurance that management and accountability arrangements are adequate, and are informed in a timely manner of future changes to the IG agenda.

IGMAG has overall responsibility for overseeing the development and implementation of IGM. These will be subject to a periodic review and progress reports and any identified risks will be highlighted to the Q&R Committee.

A key function of the IGMAG is to monitor and review untoward occurrences and incidents relating to IG and ensure that effective remedial and preventative action is taken.

The Group is responsible for scoping and developing education on IG for all Trust staff and communicating IG developments and standards to appropriate committees, forums and groups.

Information Asset Register (IAR)

All IA of the Trust should be identified and have a nominated Information Asset Owner (IAO). Accountability for assets helps to ensure that appropriate protection is maintained and any risks to data loss minimised.

Data Privacy Impact Assessments (DPIA) are performed if appropriate and these are reviewed internally and added to the IAR.

Information Asset Owners (IAO)

Their role is to understand what information is held, what is added and what is removed, how information is moved, who has access and why. They are able to understand and address risks to the information assets they 'own' and to provide assurance to the SIRO.

Information Asset Administrators (IAA)

IAA work with an IA. They ensure that policies and procedures are followed, recognise actual or potential security incidents; consult their IAO on incident management.

All Trust Employees

All Trust employees and anyone else working for the Trust (e.g. agency staff, honorary contracts, management consultants etc.) who use and has access to Trust information must understand their personal responsibilities for IG and comply with UK law.

IG Policies

All IG Policies are approved by IGMAG as a delegated group and ratified by the Trust Board. This is in accordance with the Trust's Policy P_CoG_04 'An organisation-wide Policy for the Development and Management of Policies and Procedural Documents'.

Existing policies are updated and new policies introduced in line with the current IG agenda. These policies provide the Trust Staff Code of Conduct and must be read in conjunction with staff employment contracts.

Policies outline scope and intent and provide staff with a robust IG framework whilst setting out their responsibilities as employees of the Trust. The Trust is committed to ensuring that all staff and those working with the Trust are familiar with the Trust's objectives and what is expected of staff in order to achieve these objectives.

Corporate governance processes help the Trust to assure the quality of our business and provides a framework to help the organisation achieve objectives and meet correct standards of accountability and integrity.

Contracts

C21 Patient Confidentiality, Data Protection, Freedom of Information and Transparency

Information Governance – General Responsibilities

<https://www.england.nhs.uk/wp-content/uploads/2018/05/6-nhs-standard-contract-2017-19-general-conditions-shorter-form-june-2018.pdf>

SMART CARD AND ID CARDS

The Registration Authority (RA) acts on behalf of the Trust under a Service Level Agreement (SLA) in relation to Smartcards, Care Identity Service (CIS) and ID Cards and has organisational authority for ensuring that all aspects of registration and identity card services are performed in accordance with local and national policies and procedures. It is responsible for providing arrangements that will ensure tight control over the issue and maintenance of Smartcards and identity cards, whilst providing an efficient and responsive service that meets the needs of the Trust.

Roles and Responsibilities

What is the RA?

It consists of the RA Manager, RA Agents, Local RA Agents, RA Sponsors and Smartcard Administrators.

The RA has organisational authority for:

- Ensuring that all aspects of registration and access control of Smartcard services are performed in accordance with local and national policies and procedures.
- Providing arrangements to ensure there is tight control over issuing and maintaining Smartcards.
- Providing an efficient and responsive service that meets the needs of the organisations that it supports.
- The RA operates within the governance framework identified in *Registration Authorities: Governance Arrangements for NHS Organisations* (Feb 2016) and *Registration Authorities Process Guidance*.

Role of the RA

Ensures that people providing healthcare services to the NHS directly, or indirectly, have access to NHS CRS compliant applications/information in accordance with their role

- Processes all Smartcard applications and changes
- Ensures that all forms and E-forms are appropriately used
- Ensures that resources are appointed and available to operate the registration process in a timely and efficient manner to meet the organisation's responsibilities
- Ensures that RA, Sponsors and Smartcard Administrators are adequately trained, are familiar with local and national RA procedures and have access to guidance
- Ensures that the national and local registration processes are adhered to, including the *Registration Authority Process Guidance*, *NHS Confidentiality Code of Practice* and the *Care Record Guarantee*
- Ensures that there are sufficient Smartcards, Smartcard printers and other relevant equipment for the Trust

Smartcards

A Smartcard is a plastic card that uses chip and PIN security, to give an authorised user access to clinical systems and the SPINE. A person's access is based upon their job role/s and business functions/activities, referred to as Position Based Access Control (PBAC).

The chip stores a Unique User Identifier (UUID), providing a secure link between systems and the database holding the Smartcard holder's information and access rights. The combination of the Smartcard and the password helps to protect the security and confidentiality of patients' personal and healthcare information.

As new systems are deployed, staff will be identified, their roles and access requirements agreed, and arrangements made for them to be issued with a Smartcard.

The Registration Process

The Registration process consists of three distinct activities:

1. An applicant is sponsored for a Smartcard, has their identity checked to e-Gif level 3. A personal details record is created on the CRS Spine
2. Appropriate access is granted to NHS CRS applications via one or more positions. The position must be approved by a Sponsor and granted by a RA Agent or RA Manager
3. A Smartcard is created with a passcode to link the holder to their Spine record and access profile. Access to NHS CRS application is enabled

Responsibilities for new Smartcard holders

Smartcard holders must be made aware of, and accept, the responsibilities relating to Information Governance (IG) and NHS Smartcard Terms & Conditions, during the registration meeting, or later on the National Portal. The holder is then responsible for the use and maintenance of their Smartcard

All holders issued with a Smartcard must adhere to:

- The Smartcard Terms & Conditions
- The NHS Confidentiality Code of Practice
- The Data Protection Act 2018
- Trust policies on confidentiality, information security and information sharing

The RA Sponsor must discuss Smartcard care with any holder that frequently misplaces or damages their Smartcard.

Training

All RA managers, RA agents, Local RA Agents and Sponsors need to complete the IG training modules appropriate for their job role on an annual basis. In addition to training, all individuals with RA responsibilities should have access to up to date guidance and web-based materials.

Duties

Title	Responsibilities
RA Agents	Ensure all forms are processed within agreed timescales. Record all access to local or national systems where required.
RA Sponsor	Responsible for approving, where appropriate, the registration and profiles to be granted to users. Informing the RA of user requirements/changes in a timely manner. Ensuring all ID checks comply with EGif3 standards as part of the registration process. Comply to the procedures set out in the Sponsor Guide Ensuring all actions comply with IG practices & policies.
Smartcard Administrator	Assist other smartcard users with duties documented in the guidance. Comply with the procedures set out in the Guidance Ensuring all actions comply with IG practices & policies.

Leaving/Changing Job

A smartcard is designed to stay with an individual for as long as they need it, as such should they leave a position or a Trust they should **keep** their card provided they are going to another role within the NHS or outside the NHS but using a smartcard; access must however be removed via a 'Modify Person' request within CIS where applicable.

If the new employment does not require a Smartcard then the Smartcard should be given to the manager before leaving for secure destruction by the RA as part of the Employee Leaver Process.

It is the responsibility of the Sponsor to ensure that users who leave or take an agreed period of leave from the Trust have their status recorded by the RA Dept. RA will process leavers/absentees in line with locally developed procedures, either suspending or revoking access. It is the Sponsor's responsibility to notify the RA of any users who require their Smartcard to be re-activated.

Identity Cards

ID cards must be visibly worn at all times whilst at work, whether on NHS premises or in the community; they should not be worn outside of working hours. ID cards must conform to current layouts and specifications.

The image on the cards must always be an accurate likeness of the individual, should this change a new card should be applied for and an updated picture supplied.

For users concerned about having their full name on their card, i.e. receptionists and secure unit employees cards can be double sided to allow for one face to omit their surname.

Why you need one

ID cards must be worn at all times when on duty to enhance the safety of staff and patients. Failure to wear a valid ID card may result in staff members not being able to access some sites for security reasons. It is the responsibility of all managers to ensure that their staff has a valid ID card at all times.

How to Apply

ID card applications and changes are via the IDF01 form which can be posted however, e-mail applications are preferred. Applications must be made by each staff member's manager.

Expired Cards

Once a card has expired, i.e. its two year life has been reached; the card should be securely destroyed on site or returned to the RA dept. Staff should have a valid ID card at all times and a replacement card must be requested via an IDF01 prior to the expiry date.

Leaving / Changing Job

If a cardholder changes name or their job title they need to apply for a new ID card. Once they have received the new ID card, the old one will need to be destroyed securely. Alternatively, return it to the RA Department for secure destruction.

Once a user has left the position / Trust the ID card must be handed in to the person's manager for them to either securely destroy on-site or returned to the RA Department for secure destruction.

Should a staff member be dismissed, any ID cards must be retained by the manager and returned to the RA department for destruction or shredded in line with Trust Policy.

Lost or Stolen Cards

The user should inform their line manager immediately and complete a Datix. An IDF01 (for ID cards), will then need to be completed and/or a CIS Re-Issue smartcard request (for smartcards) and submitted to the RA department so a replacement card can be provided as soon as possible. **All smartcard loses should be reported immediately to avoid misuse.**

Incident Reporting

All members of staff are encouraged to report incidents involving the use and abuse of Smartcards and identity cards. These should be reported in line with the Trusts Incident Reporting or Whistleblowing Policies.

Examples of incidents are:

- Smartcard or application misuse
- Loss or Theft of a Smartcard
- Non-compliance of local or national RA policy
- Any unauthorised access of IT applications
- Any unauthorised alteration/ to or viewing of patient data

The Directorate Manager, or equivalent, or the Sponsor will consider all incidents reported to them. Any incidents considered significant will be escalated to Information Governance in collaboration with the Data Protection process depending on the nature of the incident. A significant incident is an isolated incident or a series of less significant incidents that could lead to a serious degradation of healthcare or information security.

The RA Manager and Caldicott Guardian will consider incidents reported to them and make recommendations as to whether Trust systems or working practices should be reviewed as a result.

A major breach of security will also be reported to the local service provider and through the IG SIRI Reporting Toolkit to ensure that any risks resulting from the event can be taken into account and mitigated against.

Incidents involving breaches of security must also be reported to IG by the RA Manager so that any disciplinary measures required may be taken. The HR department will contact the relevant Directorate Manager, or equivalent, who will be responsible for ensuring an appropriate and timely investigation, is undertaken in line with the Trust's Disciplinary Policy.

Confidentiality

All users issued with a Smartcard or ID Card must adhere to the Smartcard terms & conditions, NHS Confidentiality Code of Practice and the DP legislation and any Trust policies on Confidentiality, Information Security and the Disclosure of Confidential Information. Any breaches of confidentiality or misuse of the Smartcard or Identity card may result in disciplinary action being taken up to and including dismissal, in line with Trust Policy.

All actions taken by a holder logged in with a Smartcard are recorded. The actions are traceable back to that Smartcard and the audit trail can be reviewed by the IG Lead and reserves the right to carry out random checks on Smartcard audit trails as well as specific checks after reported incidents.

Security

It is the responsibility of the RA team to ensure the secure storage of RA equipment and consumables, these areas are secured by passcode security locks or swipe card entry.

All manual files will be stored in a secure area, only accessible by passcode security locks, and accessible only by those members of staff who have been given permission.

All precautions should be taken to secure all RA mobile equipment.

All actions taken by a user logged in with their smartcard are recorded, and are traceable back to that smartcard and the audit trail can be reviewed if required. This audit trail can be used to identify misuse of the smartcard from which disciplinary measures can be taken. The Trust reserves the right to carry out random checks on smartcard audit trails as well as specific checks after reported incidents. The RA team may also undertake 'spot checks'.

Smartcard Terms and Conditions

By clicking on the 'Accept Terms and Conditions' button at the bottom of this declaration, you the applicant confirm that you:

1. understand and accept that your personal data will be used as described in the "Notice to Smartcard users on the use of your personal data" above. Furthermore, you agree to provide any additional information and documentation required by the Registration Authority to verify your identity;
2. confirm that the information which you provide in the process of your application is accurate. You agree to notify your local Registration Authority immediately of any changes to this information;
3. understand and accept that the Smartcard issued to you is the property of the NHS and you agree to use it only in the normal course of your employment or contract arrangement;
4. agree that you will check the operation of your Smartcard promptly after you receive it. This will ensure that you have been granted the correct access profiles. You also agree to notify your local Registration Authority promptly if you become aware of any problem with your Smartcard or your access profiles;
5. agree that you will keep your Smartcard private and secure and that you will not permit anybody else to use it or to establish any session with the NHS Care Records Service applications. You will not share your Passcode with any other user. You will not write your Passcode down, nor use any kind of electronic storage (media or otherwise) to store it, for example by using a programmable function key on a keyboard. You will take all reasonable steps to ensure that you always leave your workstation secure when you are not using it by removing your Smartcard. If you lose your Smartcard or if you suspect that it has been stolen or used by a third party, you will report this to your local Registration Authority as soon as possible;
6. agree that you will only use your Smartcard, the NHS Care Records Service applications and all patient data in accordance with The NHS Confidentiality Code of Practice (www.dh.gov.uk) and (where applicable) in accordance with your contract of employment or contract of provision for service (whichever is appropriate) and with any instructions relating to the NHS Care Records Service applications which are notified to you;

7. agree not to maliciously alter, neutralise, circumvent, tamper with or manipulate your Smartcard, NHS Care Records Service applications components or any access profiles given to you;
8. agree not to deliberately corrupt, invalidate, deface, damage or otherwise misuse any NHS Care Records Service applications or information stored by them. This includes, but is not limited to, the introduction of computer viruses or other malicious software that may cause disruption to the services or breaches in confidentiality;
9. understand and accept that your Smartcard may be revoked, or your access profiles changed at any time without notice if you breach this Agreement; if you breach any guidance or instructions notified to you for the use of the NHS Care Records Service applications or if such revocation or change is necessary as a security precaution. You also understand and accept that if you breach this Agreement this may be brought to the attention of your employer (or governing body in relation to independent contractors) who may then take appropriate action (including disciplinary proceedings and/or criminal prosecution);
10. understand and accept that the Registration Authority's sole responsibility is for the administration of access profiles and the issue of Smartcards for the NHS Care Records Service applications. The Registration Authority is not responsible for the availability of the NHS Care Records Service applications or applications which use NHS Care Records Service authentication or the accuracy of any patient data;
11. understand and accept that you, or your employer, shall notify your local Registration Authority at any time should either wish to terminate this Agreement and to have your Smartcard revoked e.g. on cessation of your employment or contractual arrangement with health care organisations or other relevant change in your job role;
12. understand and accept that NHS Digital may change the terms of this Agreement from time to time; and
13. understand and accept that these terms and conditions form a binding Agreement between yourself and those organisations who have sponsored your role(s). You also understand and accept that this Agreement is governed by English law and that the English courts shall settle any dispute under this Agreement.

References:

1. NHS Care Records Service applications includes the following : EPS, GP to GP, GPES, GPSoC, NHS e-RS, SCR, SUS+, Spine CIS.
2. Directions mean "the Health and Social Care Information Centre (Spine Services) (No.2) Directions 2014", and the "Novation of Information and Technology Contracts" from DH to NHS Digital: "Electronic Prescription Service, Health and Social Care Network, N3, NHS Choices, NHS e-Referral Service, Secondary Uses Service (SUS), Spine (Named Programmes) Directions 2016".

FREEDOM OF INFORMATION AND ENVIRONMENTAL INFORMATION REGULATIONS

The Freedom of Information Act 2000 (FOIA) is part of the Government's commitment to greater openness in the public sector, a commitment supported by the Trust. The FOIA will further this aim by helping to transform the culture of the public sector to one of greater openness. A right of access to information helps to make public authorities accountable and therefore limit the risk of maladministration or complacency.

The FOIA replaces the non-statutory *Code of Practice on Openness in the NHS*.

The FOIA grants two distinct rights to 'any person':

- A. A right to receive confirmation or denial that information is held by a public authority;
- B. A right of communication of that information by the public authority subject to certain conditions and exemptions. In cases where information is exempt from disclosure, except where an absolute exemption applies, a duty on public authorities to communicate with the applicant as to why the information is being withheld.

The main features of the Act are:

- a general right of access to recorded information held by public authorities, subject to certain conditions and exemptions;
- a duty on public authorities to inform the applicant whether they hold the information requested and communicate the information to them, subject to certain conditions and exemptions;
- The provisions are fully retrospective, meaning, that if the organisation holds the information when the request is received, it must be provided, subject to certain conditions and exemptions.
- The Act states that requests for information under the General Rights of Access must be received in writing and include the name of the applicant, an address for correspondence, and a clear description of the information requested. This includes email, which is the preferred method of correspondence for the majority of FOI enquirers.
- a duty on every public authority to adopt and maintain a Publication Scheme.
- the establishment of the Information Commissioner Office (ICO) with wide powers to enforce the rights created by the Act and to promote good practice together with an Information Tribunal;
- a duty on the Lord Chancellor to establish Codes of Practice for guidance on specific issues, such as Records Management (Ref 3)

Publication Scheme and Guide to Information

Section 19 of the Act makes it the duty of every public authority to adopt a Publication Scheme.

The Trust has adopted the Model Publication Scheme issued which gives an overview of the information that the organisation publishes and intends to publish in the future. It details the format in which the information is available and whether or not a charge will be made for the provision of that information. The Trust's compliance with the requirement to publish information as set out in the ICO Definition Document for Health Organisations will be regularly reviewed by the FOI Lead in accordance with ICO guidelines.

Publication scheme includes a requirement to publish datasets which have been requested and any updated version. Information in the Publication Scheme will be made automatically and proactively available. In most cases information which is made available via the Publication Scheme will be downloadable from the website. In the event that an enquirer is unable to download the information, applications for the information to be supplied in another format may be made verbally or in writing.

The Trust's Publication Scheme is available on the website
<https://www.lincolnshirecommunityhealthservices.nhs.uk/about-us/freedom-of-information>

The scheme is subject to regular review in terms of content and will be formally reviewed by the IC at regular intervals.

Scope

Procedures will apply to all Trust employees and to Non-Executive Directors and will provide a framework within the Trust to ensure compliance with the requirements of the FOIA.

Although the procedures do not apply to independent contractors, they may adopt them as they are also subject to the requirements of the FOIA.

Environmental Information Regulations 2004

The Trust recognises that, in addition to the Act, there is also an obligation on public authorities to respond to requests for environmental information under the Environmental Information Regulations (EIR) 2004.

The Trust will, as far as possible, respond to requests for environmental information using the same procedures as for responding to Freedom of Information (FOI) requests, while recognising that there are some differing regulations between EIR and FOI on the provision of information. These include rules governing what environmental information may be disclosed (exceptions under EIR) and the requirement to respond to requests for environmental information **whether the request is verbal or in writing.**

Principles

The Trust aims to create a climate of openness and dialogue with all stakeholders and improved access to information about the Trust.

This does not overturn the duties of confidence or statutory provisions that prevent disclosure of PCD. The release of such information is still covered by the subject access provisions of the DP legislation.

The Trust believes that public authorities should be allowed to discharge their functions effectively.

This means that the Trust will use the exemptions contained in the FOIA where an "absolute exemption"¹ applies or where a "qualified exemption"² will nevertheless have to be disclosed unless it can be successfully argued that the public interest in withholding it is greater than the public interest in releasing it.

¹ *the public authority may withhold the information without considering any public interest arguments e.g. Information accessible to applicant by other means*

² *information which falls into a particular exemption category, e.g. defence but where the "public Interest test" may apply*

Statement

The Trust will use all appropriate and necessary means to ensure that it complies with the FOIA and associated Codes of Practice issued by the Lord Chancellor's Department pursuant to sections 45(5) and 46(6) of the FOI Act.

Aims and Objectives

This has been developed in order to:

- ensure the Trust complies with the requirements of the FOIA;
- describe the management and accountability arrangements for the FOIA within the Trust and to provide guidance for implementing the procedures;
- ensure training and awareness sessions are provided for all employees regarding the FOIA

Accountability and Responsibilities

The Trust recognises its responsibilities to implement in full its duties in respect of the FOIA and to ensure all its employees understand and implement FOIA requirements.

Chief Executive

The Chief Executive has overall responsibility for the performance of the Trust in respect of the FOIA. The Chief Executive is therefore responsible for ensuring the implementation of the FOIA and principles by the Trust.

FOI Lead

The Trust's nominated FOI Lead is provided under an SLA with Arden & GEM CSU, who will have delegated functions to formulate the procedures, advise on FOI and on access requests and exemptions and be the focus point for the receipt of all requests under the FOIA and EIR.

Executive Directors

Executive Directors will be the focal point within each Directorate for the provision of any information requested under the FOIA and will have clear responsibilities to facilitate the gathering of all information within specific timescales. Directors are responsible for ascertaining whether information can or should be released to the public and for adjudicating in any appeals hearings against any non-disclosure complaint.

Managers

Managers at all levels are responsible for ensuring that the staff, for who they are responsible, are aware of and adhere to are updated in relation to this.

Responsibilities of all Staff and Non-Executive Directors

All staff and Non-Executive Directors are obliged to adhere to this Policy. Staff are responsible for ensuring that they identify and report access requests to the Information Governance Lead within the strict time frames. Staff are also responsible for assisting the public to complete and submit access requests wherever possible.

Training

The FOI Lead will work with the Managers to ensure that training and awareness sessions relating to the FOIA are available to staff and Non-Executive Directors who require it.

Charges and Fees

Charges and fees will only be levied in exceptional circumstances, for example where large volumes of hard copy materials are requested, in which case the Trust will follow the Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004.

In general, no charge will be made.

Time Limits for Compliance with Requests

The Trust will establish systems and procedures to ensure it complies with the duty to respond to requests within 20 working days of receipt of a request, in accordance with Section 10 of the Act. All staff will be required to comply with the requirements of these procedures. This timescale can be extended to maximum of 40 working days if the Trust is considering an exemption.

Re-use of information

The Re-use of Public Sector Information Regulations 2005 provides a framework for public sector organisation to license the re-use of their information, including the possibility of levying charges for re-use.

In providing information under the FOIA this does not give an automatic right to re-use it. "Re-use" means the use by a person of a document held by a public sector body for a purpose other than the initial purpose for which the document was produced. An example of this might be a private sector company wanting to re-publish the Trust's documents on their website as part of a commercial service.

A request for re-use will need to be in writing, state the name of the applicant, an address for correspondence, specify the document requested and state the purpose for which the document is to be re-used. The Trust will respond to a request for re-use within 20 working days of receipt (beginning with the day after receipt).

A database of requests for re-use licences will be maintained by the FOI Lead to ensure that licences are re-issued if required once lapsed.

Complaints/Internal Review

Requests for review or complaints about handling of applications for information under the Act are specifically exempt from the NHS Complaints Regulations (NHS Complaint Regulations Part II, para 7(g)).

Datasets and Re-use of information

Section 102 of the Protection of Freedoms Act 2012 adds new provisions to the FOIA regarding datasets.

The new provisions are about how information is released and relate to information the Trust holds as a dataset, which is a defined term in the new provisions.

If the Trust is providing information that constitutes a dataset and the requester has expressed a preference to receive the information in electronic form, the Trust must provide it in a re-usable form as far as reasonable practicable.

The FOIA gives a right of access to information but not the right to re-use it and datasets can be licensed for re-use. The dataset provisions do not only create a duty under s 11(1A) for the Trust to provide datasets in a form that is technically 'capable of re-use', but also a duty under s11A (2) to provide datasets that are relevant copyright works under a license that permits re-use.

However, those provisions do not remove those rights; third party rights need also be taken into consideration

In accordance with the s45 code of practice and the recommendation of the UK Government Licensing Framework the Trust will grant re-use under the Open Government License (OGL) for datasets that can be re-used without charge. It is also the default licence for Crown Copyright works.

Public Interest Test

The public interest will be considered in every case where a qualified exemption may apply. When applying the public interest test in the FOI context it means the public good, not what is of the interest to the public, and not the private interests of the requester.

In carrying out the public interest test the Trust should consider the circumstances at the time of the request or within the normal time of compliance.

Public interest arguments for the exemption must relate specifically to that exemption and the organisation must consider the balance of public interest in the circumstances of the request.

When considering the public interest to reach a decision on a qualified exemption, the organisation will seek legal advice when necessary. The Trust will aim to use the qualified exemptions sparingly and will, in accordance with Section 17 of the Act, justify their use

Requests that require additional analysis /advice or support

The following are examples that may require the need to seek additional intervention.

- Where the information would cost more than the maximum of £450 (calculated at £25 per hour for labour costs)
- Where the applicant requests an Internal Review following a refusal.

Freedom of Information (FOI) Appeals (Internal Review) Procedure

And

Appeals Panel Terms of Reference

Introduction

The right to appeal is a fundamental part of the FOIA and the EIR. This right can be exercised in two ways: by an internal review using the Trust's appeal procedures and by an external appeal to the regulator the ICO. They will not usually investigate any appeal which has not been thoroughly investigated through the organisation's internal process.

Dissatisfied applicants therefore have the opportunity for an initial review of how their request for information was handled. Having gone through this process, applicants who are still unhappy can complain to the ICO and will be dealt with in accordance with the ICO procedures.

Freedom of Information (FOI) Internal Review Procedure

Appeals must be submitted in writing within 40 days after receiving Trust's response. After this time period, the organisation will not hear appeals and applicants will be advised to contact the ICO directly.

On receipt, the request for internal review will be acknowledged before it is assigned to one of a panel of reviewers, who are usually senior members of staff, including the SIRO. The FOI Lead will provide the reviewer with a summary and details of the original handling of the request. The job of the internal reviewer is threefold:

1. To assess whether the Trust has complied with its responsibilities under the FOIA, including timeliness and the duty to advise and assist.
2. To consider the information released against the information requested and make a full review of the papers associated with the original application, if appropriate, discussing the decisions with staff who dealt with the initial application.
3. To re-consider any public interest in disclosure and determine whether the information should be disclosed.

The internal review constitutes a fresh inquiry into the request, rather than taking as a starting point the decision already reached and submitting it to a test of reasonableness. Reviews are also undertaken in the light of the general presumption in the FOIA in favour of release of information.

Useful procedural guidance and advice on the application of the exemptions can be obtained from the FOI Lead or the ICO. The ICO recommends that an internal review should take no longer than 20 working days.

The internal reviewer sets out their decision in the form of a document outlining their conclusions and recommendations. Following management approval, the outcome of the review is communicated to the applicant.

On completion of the review, records relating to the review are returned to the FOI Team. They are retained in order to assist in any investigation by the ICO.

NHSLA Monitoring

Minimum requirement to be monitored	Process for monitoring e.g. audit	Responsible individuals/ group/ committee	Frequency of monitoring /audit	Responsible individuals/ group/ committee (multidisciplinary) for review of results	Responsible individuals/ group/ committee for development of action plan	Responsible individuals/ group/ committee for monitoring of action plan
DSPT Standards	Review / Audit / Reports	IG Lead	Annual	IG Lead / IGMAG	IG Lead / IGMAG	IG Lead / IGMAG

Equality Analysis

A.	Briefly give an outline of the key objectives of the policy; what it's intended outcome is and who the intended beneficiaries are expected to be	To provide clear and effective management and accountability structures, governance processes, documented policies and procedures, a comprehensive IG training programme and adequate resources to manage and embed IG throughout the Trust.		
B.	Does the policy have an impact on patients, carers or staff, or the wider community that we have links with? Please give details	All Staff and Service Users		
C.	Is there is any evidence that the policy\service relates to an area with known inequalities? Please give details	No		
D.	Will/Does the implementation of the policy\service result in different impacts for protected characteristics?	No		
		Yes	No	
	Disability		X	
	Sexual Orientation		X	
	Sex		X	
	Gender Reassignment		X	
	Race		X	
	Marriage/Civil Partnership		X	
	Maternity/Pregnancy		X	
	Age		X	
	Religion or Belief		X	
	Carers		X	
	If you have answered 'Yes' to any of the questions then you are required to carry out a full Equality Analysis which should be approved by the Equality and Human Rights Lead – please go to section 2			
The above named policy has been considered and does not require a full equality analysis				
Equality Analysis Carried out by:		Kaz Scott		
May 2018		June 2018		