NHS
Medway
NHS Foundation Trust

Information Governance Strategy

Author:	Information Governance Officer- Rachel Adams
Document Owner	Trust Secretary and Director of Corporate compliance and Legal service, Sheila Murphy
Revision No:	9
Document ID Number	STRCGR013
Approved By:	Information Governance Group
Implementation Date:	June 2018
Date of Next Review:	June 2019 (annual review)

Best of care
Best of people

Document Control / History	
Revision No	**Reason for change**
2	NHSIA Toolkit became the Connecting For Health IG Toolkit Version 4 in September 2006
	HSC 1999/053 was renamed to Records Management: NHS Code of Practice
	Membership and Responsibilities changed due to change in Organisational Structure
3	Regular review
4	Responsibilities and Terms of reference changed due change in reporting arrangements and structure
5	2 yearly review
6	2 yearly review. Change of roles and reporting Committee
7	Separation of IG Policy from Strategy document
8	Annual review of strategy
9	Annual review of strategy

Consultation
Information Governance Group members

Table of Contents

1 Introduction

1.1 This strategy sets out the approach adopted at Medway Foundation Trust to provide a robust Information Governance (IG) Management Framework, for the current and future management of information, and compliance with required legislation.

1.2 Any associated resource implications incurred by the implementation of the IG Strategy, will be identified by the IG Group, and reported to the Trust's Board as appropriate and required.

1.3 This strategy sets out how the Trust can further develop and implement a change in culture towards IG by all staff. IG is a key component of performance management, i.e. it is central to the working practice of all staff, levels and roles, permanent or temporary, within the Trust.

1.4 Through the implementation of the IG Strategy, the Trust will:

- establish robust information governance processes conforming to the law, NHS Digital requirements and guidance by the Information Commissioners Office (ICO)
- ensure that all policies and procedures relating to the processing of personal information, including handling and holding personal and Trust corporate information are legal and conform to best and/or recommended practice;
- ensure that clear information is given to patients, families and carers, and staff about how their personal information is recorded, handled, stored and (if required) shared by the Trust. The public will be provided with guidance, available in various formats, to explain their rights, how their information is handled, how they can obtain further information and how they can raise concerns. This is published in the Privacy Notices that are available on the Trust's website.
- provide clear advice and guidance to staff and ensure that they understand and apply the principles of Information Governance to their working practice in relation to protecting the confidentiality and security of personal information and to ensure the safekeeping and handling of the Trust's business information, and compliance with appropriate legislation.
- ensure that procedures are reviewed on a regular basis to monitor their effectiveness in order for improvements or deficiencies in information handling standards to be recognised and addressed to embed an Information Governance culture in the Trust through increasing awareness and providing training on the key issues.
- maintain a clear reporting structure and ensure that through management action and training all staff understand the IG requirements.
- undertake regular reviews and audits of how information is recorded, held and used. Audits will be used to identify good and bad practice.
- ensure that there are robust procedures for notifying and learning from IG breaches and incidents in line with the Data Security and Protection Breach Notification national guidance and Trust SOP which is available via QPulse.
- ensure improvement plans are developed and agreed in response to the Data Security and Protection Toolkit (DS&P), developing and taking forward improvement

plans pertaining to the current toolkit, and reporting progress to the Information Governance Group on a regular basis.

- ensure that the National Data Security Standards are embedded in the IG culture, including continuing to highlight and manage/mitigate risks to cyber security.

2 Current Position (where we are now)

2.1 Following the departure of the Information Governance Manager at the end of December 2017, the IG components were separated into Subject Access requests, Freedom of Information and Information Governance

2.2 The Trust has a published compliance status of 'satisfactory' against version 14.5 of the IG Toolkit requirements in March 2018, based upon an honest and robust assessment of compliance conducted in 2017-18 which was reviewed by our internal auditors KPMG in November 2017.

2.3 The new Data Protection and Security toolkit (DS&P) was published on the 1 April 2018. This has been radically redesigned and is now in-line with the 10 National Data Guardian (NDG) standards and along with the changes in legislation means the majority of evidence and policies previously used are now null and void. |The Information Governance team have created a working party with IT, BI, HR and Health Records to review the requirements and ascertain what information the Trust already holds and what needs to be created.

2.4 The Transparency agenda under FOI has improved with the:

- pro-active publication of FOIA requests and responses on the Trust's website. The Trust's FOIA performance is also published on the website on a quarterly basis; and
- Trust's Publication Scheme which is being reviewed regularly and departments are being encouraged to proactively publish information if appropriate.

2.5 The uptake for Data Security awareness training/Information Governance Training as at the 30 May 2018 stands at 85% with the National target of 95%. This is despite the IG team running monthly sessions and also offer bespoke training sessions for teams. The training is also available on-line and available via the @MFT app.

2.6 Due to the change in structure the projects planned for 2017-18 have not been completed and will be moved forward to 2018-19. This includes data flow mapping, implementation of the Information Asset Owner group and a review of Corporate Record Keeping.

2.7 With the help of Hill Dickinson LLP the Trust has reached the minimum requirement to become GDPR compliant - this includes:

- appointment of a Data Protection Officer/ Accountable Officer
- review of the Trusts website

- review of the Trust privacy notices and creation of new ones for children, careers and members and governors
- policy updates
- senior management training
- data flow mapping (minimum returns)

2.8 IG risks are managed through a robust framework and reviewed at a minimum on a quarterly basis by the Information Governance Group. Escalated risks are reviewed by the Trust's Executive Group.

3 The Vision (where we want to be)

3.1 The Information Governance team has 7 designated work streams for 2018-19:

- **DPO work stream - this includes but is not limited to:**
  - ensuring the Trust stays GDPR compliant
  - ensuring privacy statements are kept up to date
  - answering GDPR/ DPA 2018 questions from any individual (including patients and staff)
  - coordinating and managing the 8 rights of individuals (please note the right of subject access is now organised separately from the IG function, however ICO complaints is still monitored through the team)
  - monitoring the DPO email box and designated phone line
  - data sharing
  - manual audits i.e. ward checks
  - ensuring the Trust is kept up to date with changes in legislation
  - liaison with the Information Commissioners Office (ICO)
  - liaison with other organisations in relation to data sharing
  - managing incident reporting and dissemination of lessons learnt
  - coordinator for privacy impact assessments
- **SIRO work stream - this includes but is not limited to:**
  - creation and running of the Information Asset owner group
    - audits of electronic systems
    - assurance of IG compliance within departments
  - information risk management

- **DS&P Toolkit/ NDG work stream - this includes but is not limited to:**

  - collecting information from internal partners for the new 10 Data Security standards (for overview see Appendix 1)
  - ensuring compliance updates are provided through the Board to external organisations i.e. NHS Improvements
  - ensure the Trust achieves a satisfactory Toolkit submission
  - ensure the Trust is internally audited via KPMG

- **Training - this includes but is not limited to:**
  - the Information Governance team runs a number of different training courses throughout the year (please see Appendix 2 for more detail)
- **Communications internal and external - this includes but is not limited to:**
  - the IG team creates and circulates regular updates internally and now has a number of pages on the intranet for the planned updates (see Appendix 3)
- **Corporate Records - this includes but is not limited to:**
  - the project was originally started in 2017/18 however due to lack of capacity this was not completed.
  - The IG team are creating a work plan for 2018/19
- **FOI/publication scheme and transparency - this includes but is not limited to:**
  - improving the Trust's performance on responses
  - Improving the transparency of the Trust by proactive publication of Information.

The IG team is also working with other teams internally and externally to ensure:

- the national opt-out programme is implemented
- the review and culling of clinical records currently stored at Sterling Park is being managed effectively and in accordance with the Trust's Overarching Records Management and Lifecycle Policy
- GDPR compliance with IT upgrades and new system implementation
- Ensuring the Medway Hospital Charity is GDPR compliant

4 Sustainability (the do nothing gap)

4.1 The introduction of the new DS&P toolkit means the Trust will need to start collating information from scratch. Failure to do so will lead to the DS&P failing in March 2019.

4.2 Failure to pro-actively maintain a robust Publication Scheme that does not meet current ICO best practice standards will mean the Trust will fail the transparency requirement of public bodies.

4.3 Failure to maintain an effective Disclosure Log and Publication Scheme could also lead to increased FOIA requests where members of the public cannot find information that we are required to routinely publish.

4.4 Failure to be compliant with the GDPR exposes the Trust to the GDPR's increased fines regime – fines increased to a maximum of €20m or 4% of the gross annual turnover of the Trust whichever is greater.

4.5 Failure to achieve these elements collectively presents further reputational risk to the Trust.

4.6 Failure to appoint to the Information Governance structure will lead to the Trust failing an internal audit as there is no resilience in the team.

5 Governance Overview (measuring & monitoring)

5.1 IG risks are monitored by the relevant risk owner and reviewed by the Information Governance Group (IGG) on a quarterly basis and escalated to the Executive Group by the DPO where necessary.

5.2 DS&P toolkit compliance is reviewed at each IGG meeting to evidence progression throughout the year. This is audited annually by our internal auditors KMPG.

5.3 Compliance with the GDPR is monitored by the DPO and reported via the IGG.

5.4 The Trust has a KPI of 85% compliance in terms of timely disclosure under the Subject Access Provision of the Act and the Access to Health Records Act. This is now led by Legal Services. However this functions still provides reports to the IGG quarterly.

5.5 The Transparency agenda is measured and evidenced through two channels:

- the pro-active publication of FOIA requests and responses on the Trust's website. The Trust's FOIA performance will be published on the website on a quarterly basis; and
- effective maintenance of the Trust's Publication Scheme through regular audit and engagement with Owners and Publishers.

The KPI for FOI requests is 95% as set by ICO.

6 Values and Principles (values that underpin the system)

6.1 The Trust aims to 'Be the BEST' in everything it sets out to do, and this extends to:

- embedding IG at the heart of how it protects, manages and uses both patient and staff personal information, and
- Being an exemplar in its transparency in public business.

7 Financial Implications (cost)

7.1 Under the GDPR the fines have increased to a maximum of €20m or 4% of the gross annual turnover of the Trust whichever is greater.

7.2 Failure to comply with Information Governance legislation can also lead to reputational damage, leading to:

- Failure of public bodies to engage in data sharing and shared service activities with the Trust

- Failure of the Trust to attract and retain the right workforce, which, as a result, will place a reliance on more expensive interim and agency staff

8 References

Document	Ref No
References:	
NHS Digital Data Security and Protection toolkit (DS&P)	
General Data Protection Regulations (GDPR)	
Freedom of Information Act 2000	
Information Security Management ISO 27001:2005	
Records management: IGA code of practice	
The NHS Confidentiality Code of Practice	
Trust Associated Documents:	
Information Governance Policy	POLCGR017
Information Governance Framework	OTCGR141
Information Governance transfer and storage of Information SOP	GUCGR022
Records Management and Lifecycle Strategy	POLCGR059
All IM&T policies Records Management Policies	
Data Protection Policy	POLCGR007
Freedom of Information	POLCGR009

END OF DOCUMENT

Data Security Standards Appendix 1

Standard 1	All staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form. Personal confidential data is only shared for lawful and appropriate purposes. Staff understand how to strike the balance between sharing and protecting information, and assistance is on hand to help them make sensible judgments. Staff are trained on the relevant requirements of legislation and periodically reminded of the consequences to patients, their employer and to themselves of mishandling personal data.
Standard 2	All staff understand their responsibilities under the National Data Guardian's Data Security Standards, including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches. All staff understand what constitutes deliberate, negligent or complacent behaviour and the implications for their employment. They are made aware that their usage of IT systems is logged and attributable to them personally. Insecure behaviours are reported without fear of recrimination and procedures which prompt insecure workarounds are reported, with action taken.
Standard 3	All staff complete appropriate annual data security training and pass a mandatory test, provided linked to the revised Information Governance Toolkit. All staff complete an annual security module, linked to 'CareCERT Assurance'. The course is followed by a test, which can be re-taken unlimited times but which must ultimately be passed. Staff are supported by their organisation in understanding data security and in passing the test. The training includes a number of realistic and relevant case studies.

Standard 4	Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All access to personal confidential data on IT systems can be attributed to individuals. The principle of 'least privilege' is applied, so that users do not have access to data they have no business need to see. Staff do not accumulate system accesses over time. User privileges are proactively managed so that there is, as far as is practicable, a forensic trail back to a specific user or user group. Where necessary, organisations will look to non-technical means of recording IT usage (e.g. sign in sheets, CCTV, correlation with other systems, shift rosters etc).
Standard 5	Processes are reviewed at least annually to identify and improve processes which have caused breaches or near misses, or which force staff to use workarounds which compromise data security. Past security breaches and near misses are recorded and used to inform periodic workshops to identify and manage problem processes. User representation is crucial. This should be a candid look at where high risk behaviours are most commonly seen, followed by actions to address these issues while not making life more painful for users (as pain will often be the root cause of an insecure workaround). If security feels like a hassle, it's not being done properly.
Standard 6	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, with a report made to senior management within 12 hours of detection. All staff are trained on how to report an incident, and appreciation is expressed when incidents are reported. Sitting on an incident, rather than reporting it promptly, faces harsh sanctions. The Board understands that it is ultimately accountable for the impact of security incidents, and bears the responsibility for making staff aware of their responsibilities to report upwards. Basic safeguards are in place to prevent users from unsafe internet use. Anti-virus, anti-spam filters and basic firewall protections are deployed to protect users from basic internet-borne threats.

Standard 7	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, with a report to senior management. A business continuity exercise is run every year as a minimum, with guidance and templates available from [CareCERT Assurance]. Those in key roles will receive dedicated training so as to make judicious use of the available materials, ensuring that planning is modelled around the needs of their own business. There should be a clear focus on enabling senior management to make good decisions, and this requires genuine understanding of the topic, as well as the good use of plain English.
Standard 8	No unsupported operating systems, software or internet browsers are used within the IT estate. Guidance and support is available from CareCERT Assurance to ensure risk owners understand how to prioritise their vulnerabilities. There is a clear recognition that not all unsupported systems can be upgraded and that financial and other constraints should drive intelligent discussion around priorities. Value for money is of utmost importance, as is the need to understand the risks posed by those systems which cannot be upgraded. It’s about demonstrating that analysis has been done and informed decisions were made.
Standard 9	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. [CareCERT Assurance] assists risk owners in understanding which national frameworks do what, and which components are intended to achieve which outcomes. There is a clear understanding that organisations can tackle the NDG Standards in whichever order they choose, and that the emphasis is on progress from their own starting points.

Standard 10	IT suppliers are held accountable via contracts for protecting the personal confidential data they process and meeting the National Data Guardian's Data Security Standards. IT suppliers understand their obligations as data processors under the GDPR, and the necessity to educate and inform customers, working with them to combine security and usability in systems. IT suppliers typically service large numbers of similar organisations and as such represent a large proportion of the overall 'attack surface'. Consequently, their duty for robust risk management is vital and should be built into contracts as a matter of course. It is incumbent on suppliers of all IT systems to ensure their software runs on supported operating systems and is compatible with supported internet browsers and plug-ins.

Information Governance Training needs Analysis Appendix 2

Training Program	Frequency	Course length	Delivery method	Target area	Facilitator	Record of attendance
Data Security and awareness L1 training	Annually	1.5 hours	ELearning or classroom	New staff	Information Governance team	ESR
Data Security and awareness L1 training	Annually	1.5 hours	ELearning or classroom	All staff	Information Governance team	ESR
Data Security and awareness L1 training	Annually	1.5 hours	Classroom	Junior Doctors and student nurses	Information Governance team	ESR
Information Asset owner (IAO) training (basic)	Annually	1	Bespoke classroom based training sessions.	Designated IAO	Information Governance team	Records held by Information Governance team
Information Asset owner (IAO) and administrator (IAA) Data flow mapping (DFM) training	As and when minimum once yearly	1.5	Bespoke classroom based training sessions	Designated IAO/IAA	Information Governance team	Records held by Information Governance team
Information Asset owner (IAO) and administrator (IAA) data privacy impact assessment (DPIA)	As and when minimum once yearly	1.5	Bespoke classroom based training sessions	Designated IAO/IAA	Information Governance team	Records held by Information Governance team

Information Asset owner (IAO) and administrator (IAA) Corporate Records Management	As and when minimum once yearly	1.5	Bespoke classroom based training sessions	Designated IAO/IAA	Information Governance team	Records held by Information Governance team
Information Asset owner (IAO) and administrator (IAA) Cyber security	As and when minimum once yearly	1.5	Bespoke classroom based training sessions	Designated IAO/IAA	Information Governance team/ IM&T	Records held by Information Governance team
SIRO training	Annually	1 day course	Specialist training via external provider or NHS digital workbook	SIRO	Specialist training via external provider or NHS digital workbook	Records held by Information Governance team
Caldicott Guardian training	Annually	1 day course	Specialist training via external provider or NHS digital workbook	Caldicott	Specialist training via external provider or NHS digital workbook	Records held by Information Governance team
Data Protection Officer training	Annually	1 day course	Specialist training via external provider or NHS digital workbook	Data Protection Officer	Specialist training via external provider or NHS digital workbook	Records held by Information Governance team

Updates on legislation changes.	As and when minimum once yearly	1 hour	Bespoke classroom based training sessions	Executive Directors and Board members	Data Protection Officer	Records held by Information Governance team
Information Governance Manager and Officer - Updates on legislation changes.	As and when minimum once yearly	1 hour	Bespoke classroom based training sessions	Information Governance Manager and Officer	Specialist training via external provider or NHS digital workbook	Records held by Information Governance team
Subject access request team	Annually	1 hour	Bespoke classroom based training or NHS digital workbook	SAR team	Information Governance team	Records held by Information Governance team

Internal Communications planned for 2018/2019 Appendix 3

Month	Theme
June	Updates from the GDPR
July	Introduction to the Senior Information Risk owner (SIRO) and the Caldicott Guardian and Data Protection Officer (DPO) what they do and why they are important roles.
August	Records management – Corporate and Clinical
September	Data flows – How to complete data flows and why they are so important. Month to also include the importance of Data sharing
October	Information Governance training and Information Governance toolkit
November	Data protection breaches and cyber attacks
December	Social media and Information Governance implications
January	Refresh on what has been delivered so far.
February	Post Brexit Data Protection Act 2018– How it will affect you at work and at home
March	How to keep information safe –practical security emails, fax, clear desks etc.
April	Refresh on what has been delivered so far.
May	How to keep information safe –practical security emails, fax, clear desks etc.