Liverpool Heart and Chest Hospital NHS
NHS Foundation Trust

Reference Number: FOI/2020/211
From: Private Individual

Date: 29 July 2020

Subject: Organisational structure, systems and processes of the management of information

Q1 Who carries out the role of your Senior Information Risk Officer (SIRO) and is this a dual or stand alone role - Full Job title and name

A1 Dual role – job title and name information exempt under Section 21 of the Freedom of Information Act 2000 - 'Information reasonably accessible to the applicant by other means'.

This information is available on our website:-
https://www.lhch.nhs.uk/about-lhch/information-governance/our-team/

Q2 Who carries out the role of Chief Information Officer (CIO) and is this a dual or stand alone role - Full Job title and name

A2 Gregg Holland, Chief Information Officer – stand-alone

Q3 Who carries out the role of Data Protection Officer (DPO) and is this a dual or stand alone role - Full Job title and name

A3 Dual role – job title and name information exempt under Section 21 of the Freedom of Information Act 2000 - 'Information reasonably accessible to the applicant by other means'.

This information is available on our website:-
https://www.lhch.nhs.uk/about-lhch/information-governance/our-team/

Q4 Who carries out the role of IG Manager (or equivalent ie. Head of IG) - Full Job title and name

A4 As per A3

Q5 Questions 1 - 4 - Can we please have a copy of their job descriptions (Whether these are dual or stand alone job descriptions) and their pay banding.

A5 See attached:
Job Description SIRO - This role is a joint appointment split between Alder Hey Hospital and Liverpool Heart and Chest Hospital. As such all administration for pay purposes is handled by Alder Hey.
Job Description CIO – Pay Band 8d
Job Description DPO – Pay Band 8b
Job Description Head of IG and Admin – Pay Band 8b

Q6 Questions 1 - 4 could we please have a copy of their department structure

A6 See attached:
FOI2020211 Digital Structure
FOI2020211 Patient Admin Structure

Q7 Do you have a separate structure specifically to support SIRO/CIO in their roles?

A7 No specific structure however governance support is provided by the following roles:- Caldicott Guardian; DPO; Information Governance and Information Security Teams

Q8 Do you have an information asset structure to support SIRO, can you advise on this is not covered by the above structure chart.

A8 The Trust's information risk management structure is as follows:-

Structural Model
Accounting Officer (CEO)
Senior Information Risk Owner (SIRO)
Information Asset Owners (IAOs)
Information Asset Administrators (IAAs)
Information Asset Register (IAR)

Q9 Have you identified your information asset owners and administrators? What role do they take within your organisation (e.g. head of service level) and how are their responsibilities defined. If in a document or JD please provide a copy.

A9 Owners and Administrators have been identified, roles will vary however. Owners for instance will be senior responsible roles such Divisional Head of Operations, Heads of Service etc.

Responsibilities for owners are detailed in the Trust's Information Risk Management policy

Q10 Do you deliver a training package to your Information Asset Owners and/or administrators? How often do they do this training? If so, can we please see a copy?

A10 Trust policy is for training to be undertaken every three years; training is currently face to face local in-house training – see attached copy, however the Trust is looking to introduce e-learning developed by NHS Digital and Templar Executives Ltd.

Q11 Do you have a group where the IAO/ IAA or SIRO meet and discuss information risk and if so could I have a copy of the Terms of reference for this group.

A11 No specific SIRO/IAO/IAA group, the Trust has a Cyber Security and Information Governance Assurance Group and Digital Healthcare Committee (DHC). Risks from the Group are reported either to the DHC or Risk Management Committee and the Group completes an annual SIRO report.

TORs – see attached

- ToR Cyber Security and IG
- ToR Risk Management Corporate Governance and Health and Safety

The Digital Healthcare Committee ToR is currently under review and as such is unavailable for publication.

Q12 What software do you use to map out your information assets i.e. excel, third party solution such as One Trust, CoreStream

A12 Excel

Q13 Could I request a copy of your information asset register (template) and data flow mapping template

A13 Information not held – we do not have a template for the Information Asset Register
See attached for the data flow mapping template - Data Mapping Template v4.0

Q14 Could we please have a copy of your Data Protection Impact Assessment (DPIA) template.

Q14 See attached - DPIA template v1.3

Data Flow Mapping for:	Cheshire & Merseyside Respiratory Improvement Programme

Please list below all incoming data flows to your department. In addition, please list any access granted to another third party to any Trust systems or data e.g. to system suppliers.

For guidance please refer to the Guidance Notes tab or contact Information Governance (x1845/1240)

1. What personal-identifiable data comes into your department?										2. Where does the data come from?		3. How is the data transferred					4. Risk Assessment (To be completed by IG Team)		
1.1 Received from	1.2 Categories of personal data		1.3 Categories of data subject	1.4 Purpose of flow / data processing		1.5 Legal Basis		1.6 Frequency	1.7 Volume	2.1 Originator	2.2 Is a Formal Contract or SLA in place to support data flow?	3.1 Transfer medium	3.2 Transfer method	3.3 Safeguards in place	3.4 Is an Information Sharing or Data Processor Agreement in place?	3.5 Risks identified	Clarification question(s)	Comments	Risk level
Enter details of who you receive the data from e.g. patient; NOK; GP; NHS Hospital; Private Hospital etc.	Select from drop-down list	Please give details of specific data (name; address; DOB, Telephone No; Pay; Images; Biometric data etc.	Select from drop-down list	Select from drop-down list	Please give details for non-care purposes e.g. employment processing; statutory obligtion; recruitment assessment etc.	Personal Data Select from drop-down list	Special categories Select from drop-down list	Select from drop-down list	Select from drop-down list	Select from drop-down list	Select from drop-down list	Select from drop-down list	Please specify how the data is transferred or shared	Please specify the safeguards in place to protect the flow of data	Select from drop-down list	Please give details of the risks identified for this data flow	For completion by the IG Team		

Date completed:	
Date reviewed:	
Date reviewed:	
Date reviewed:	

Data Protection Impact Assessment (DPIA)

Part 1: Overview and screening questions (to be completed in conjunction with the IG Team – email infogov@lhch.nhs.uk to book a meeting)

Overview	
What is the project's name	Enter details
What is the proposed implementation date?	Enter details
What is the reason for the proposed change?	Give details of the background to the proposed change
What is the project's scope and terms of reference	Give details
Who are the project's key stakeholders?	List the individuals; groups or organisation that may have an interest in, a role to play in delivering, or be affected by the project
What does the project aim to achieve?	Give brief details
What benefits will the proposed change deliver?	Give details of the benefits for the Trust, its patients or other parties
Who is the project's Executive Sponsor?	Name: Job Title: Department: Phone: Email:
Who is the Project Manager responsible for implementing the change?	Name: Job Title: Department: Phone: Email:
What type of change will be involved? *Select as applicable* ☐ New service ☐ New process ☐ New software ☐ New hardware ☐ New system interface or linkage	☐ Change to existing service ☐ Change to existing process ☐ Change to existing software ☐ Change to existing hardware ☐ Change to existing system interface or linkage
What software; hardware or system interface/linkage between systems does the project involve?	Give details, if applicable
Who is the supplier/provide of the software and/or hardware?	Give details, if applicable, include the data protection fee registration number
Where is the system hosted?	Give details - state physical location of server and whether cloud based
Who supports the system (i.e. technical support)?	☐ In-house ☐ External third party - Give details
What contractual arrangements are in place	*Click on choose an item below and select from the drop down*

<table>
<tr><td>with the supplier?</td><td colspan="3">list:

Choose an item.</td></tr>
<tr><td>Who is the Trust's Information Asset Owner for the system?
For changes involving hardware/software give details of the most senior member of Trust staff accountable for the system</td><td colspan="3">Name:
Job Title:
Department:
Phone:
Email:</td></tr>
<tr><td>Who is the Trust's Information Asset Administrator(s) for system?
For changes involving hardware/software give details of the member of Trust staff responsible for day to day management of the system</td><td colspan="2">Administration
Name:
Job Title:
Department:
Phone:
Email:</td><td>Technical
Name:
Job Title:
Department:
Phone:
Email:</td></tr>
<tr><td>How many individuals will be affected by the project?</td><td colspan="3">Give details</td></tr>
<tr><td>What is the purpose(s) for the processing of personal data?</td><td colspan="3">Give details of the processing purpose(s)</td></tr>
<tr><td>Who determined the purpose(s) and means of processing the personal data?</td><td colspan="3">Give details of which organisation or organisations decided why and how the personal data will be processed</td></tr>
<tr><td>What are the categories of data subjects?</td><td colspan="3">Click on choose an item below and select from the drop down list:

Choose an item.</td></tr>
<tr><td colspan="4">What type of personal data will the project involve?
Select as applicable</td></tr>
<tr><td colspan="3">Personal data: ☐</td><td colspan="3">Special category data: ☐</td></tr>
<tr><td>Forename ☐</td><td>Surname ☐</td><td>Address ☐</td><td>Ethnicity ☐</td><td>Sexual life ☐</td><td>Religion ☐
Belief system</td></tr>
<tr><td>Post Code ☐</td><td>Age ☐</td><td>Hospital No ☐</td><td>Political ☐
opinion</td><td>Trade Union ☐
Membership</td><td>Crime / ☐
Justice issues</td></tr>
<tr><td>NHS No ☐</td><td>NI No ☐</td><td>Phone No ☐</td><td>Health ☐</td><td>Genetics ☐</td><td>Biometrics ☐</td></tr>
<tr><td>Mobile No ☐</td><td>Email ☐</td><td>Gender ☐</td><td colspan="3" rowspan="2">Other ☐ - give details (e.g. mental health; sexual health; disability status; safeguarding adults):</td></tr>
<tr><td colspan="3">Other ☐ - give details (e.g. GP name & address; Physical description; Photographs of persons; Marital status; Financial information):</td></tr>
<tr><td>What is the lawful basis under data protection law supporting the processing of personal data for the purpose(s)? Click here for details</td><td colspan="3">Click on choose an item below and select from the drop down list:
Choose an item.</td></tr>
<tr><td>What is the additional lawful basis data protection law supporting the processing of special category data? Click here for details</td><td colspan="3">Click on choose an item below and select from the drop down list:
Choose an item.</td></tr>
<tr><td>If consent is the lawful basis, what is the procedure for obtaining, recording and managing consent?</td><td colspan="3">Give details of how consent will be collected; recorded; reviewed and what happens if consent is withdrawn</td></tr>
</table>

What is the common law basis being used to support the processing of personal data	*Click on choose an item below and select from the drop down list:* Choose an item.

Screening questions	
Will the project involve the collection of new information about individuals?	If yes - list the data items to be collected
Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	If yes, give details of what data will be disclosed and who it will be sent to
Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	If yes - give details the new purpose(s)
Does the project involve you using new technology that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.	If yes - give details of the new technology
Will the project result decisions or action being taken that may have a significant impact on individuals?	If yes - give details of the potential actions and impacts
Will the project require you to contact individuals in ways that they may find intrusive?	If yes - give details of how individuals will be contacted

If the project affects more than 1,000 individuals; or involves new technology or involves high-risk processing as defined by the ICO or the answer to any of the screening questions is yes then Part Two **must** be completed.

Screening Review (for completion by Information Governance)

Date of review:	**Comments:**

Part 2: Data Protection Impact Assessment (DPIA)

DPIA questions	
How will personal data be collected?	Explain your process for collecting the data, include the source of the data e.g. from the individual; from a third party etc.
What are the data flows for the project?	Give details of all personal data flows
How will you tell individuals about the use of their personal details?	Give details of the local privacy notice process to inform patients
Which personal data could you not use without compromising the needs of the project?	Give details of what asssessment has been done regarding the adequacy, relevant and necessity for the collection of the data items
Where and in what format will the personal data be stored? *Select as applicable*	
☐ Paper local ☐ Local database ☐ Local system	☐ Paper external ☐ External database ☐ External system
What technical & organisational measures are in place to protect and secure the personal data? Please include measures to protect system interfaces/linkages. Click here for SLSP template	Give details of LHCH and supplier measures or attach a copy of the completed System Level Security Policy for the software and include staff training
Who will have access to the personal data?	Give details include LHCH staff; external suppliers etc.
How will access to the personal data be restricted?	Give details of access & user permissions and audit procedures
How will access to the personal data be audited?	Give details of procedures or where a new system is being procured or developed give confirmation it has audit trail functionality to capture details of who accesses and amends data?
How will you ensure that personal data obtained from the individuals or other organisations is accurate?	Give details of procedures
How will personal data be kept up to date and checked for accuracy and completeness?	Give details of procedures
If you are procuring or developing new software will it allow you to amend data as necessary?	Give details of how this will be done
Does the proposed change involve sending direct marketing messages by electronic means?	☐ Yes ☐ No If yes - give details:
Does the proposed change involve automated decision making?	☐ Yes ☐ No If yes give details of how individual's will be notified about the automated process: If yes, can the automated process be replaced by human intervention if required?

If you are procuring or developing new software will it allow all personal data (i.e. full records and audit trails) to be extracted to support the individuals' right of access?	Give details of the process for extracting data
What anonymisation controls are in place to support the use or sharing of data for purposes other than direct care of the individual? Click for guidance	Give details
How will requests from individuals for the processing of their data be restricted or for data to be rectified or erased be handled?	Give details of how requests will be handled and complied with, where applicable. Subject to specific circumstances as set out by the GDPR
Have potential new processing purposes been identified as the scope of the project expands?	If yes - what are new purposes, the lawful bases identified to support them and is the additiional processing compatable with the original processing purspose?
Will personal data be transferred outside the EU to another country? Click here for EU countries	Give details of the countries and the recipients of the data
If yes, how will the security and confidentiality of data be protected?	Give details of the safeguards in place to protect the data during transit and on receipt
How long will the personal data be retained for after the processing purpose has ended? Click here for retention guidance	Give details of the national NHS or statutory retention period applicable to the data and processing purpose; include data held by LHCH and the supplier
What happens when the retention period has been exceeded?	Give details of how data will be destroyed or de-personalised; cover data held by LHCH and the supplier
If you are procuring or developing new software will it allow you to delete information in line with the relevant retention period? Click here for SLSP template	Give details of how this will be done or attach a copy of the completed System Level Security Policy for the software

Part 3: Data Protection Risks and Action Plan

Potential risks and data protection issues	**Risk – Likelihood of harm**	**Risk – Impact of harm**	**Proposed solutions / action to be taken**	**Result & evaluation**	**Complete by date**	**Action to be taken by**
Give details of the associated risks to the individual data subject | the associated legal compliance | corporate risks to the Trust	*What is the likelihood of the risk happening?*	*What would be the harm / impact on the data subject / Trust?*	*Give details of the proposed actions to reduce the risks and any future steps that are necessary*	*Will the risk be eliminated; reduced or accepted and is the final impact on the individuals a justified, compliant and proportionate response to the aims of the project? Give details*	*Give details - must be before implementation / go live for the project*	*Give details of the responsible individual*
	☐1 Rare ☐ 2 Unlikely ☐ 3 Possible ☐ 4 Likely ☐ 5 Almost Certain	☐ 1 No Harm ☐ 2 Low Harm ☐ 3 Moderate ☐ 4 Major Harm ☐ 5 Catastrophic				
	☐1 Rare ☐ 2 Unlikely ☐ 3 Possible ☐ 4 Likely ☐ 5 Almost Certain	☐ 1 No Harm ☐ 2 Low Harm ☐ 3 Moderate ☐ 4 Major Harm ☐ 5 Catastrophic				
	☐1 Rare ☐ 2 Unlikely ☐ 3 Possible ☐ 4 Likely ☐ 5 Almost Certain	☐ 1 No Harm ☐ 2 Low Harm ☐ 3 Moderate ☐ 4 Major Harm ☐ 5 Catastrophic				
	☐1 Rare ☐ 2 Unlikely ☐ 3 Possible ☐ 4 Likely ☐ 5 Almost Certain	☐ 1 No Harm ☐ 2 Low Harm ☐ 3 Moderate ☐ 4 Major Harm ☐ 5 Catastrophic				

Risks and actions to be added to the overall project plan and to the appropriate corporate risk register.

Unmitigated risks must be reported to the relevant committee in line with Trust Risk Management policy (above 15 > Board; above 10 > Risk Management and Corporate Governance Committee; above 8 > Divisional Governance; below 6 Ward/Departmental management)

Part 4: Cyber Security and Information Governance Assurance Group Review

Date of review:	**Comments:**
Information Governance:	Date: enter date of review Enter review comments / give details of any additional risks identifed or substanstial risks that require a detailed risk assessment and inclusion in the formal project risk registered
IT Security:	Date: enter date of review Enter review comments / give details of any additional risks identifed or substanstial risks that require a detailed risk assessment and inclusion in the formal project risk registered
Data Protection Officer:	Date: enter date of review Enter review comments / give details of any additional risks identifed or substanstial risks that require a detailed risk assessment and inclusion in the formal project risk registered

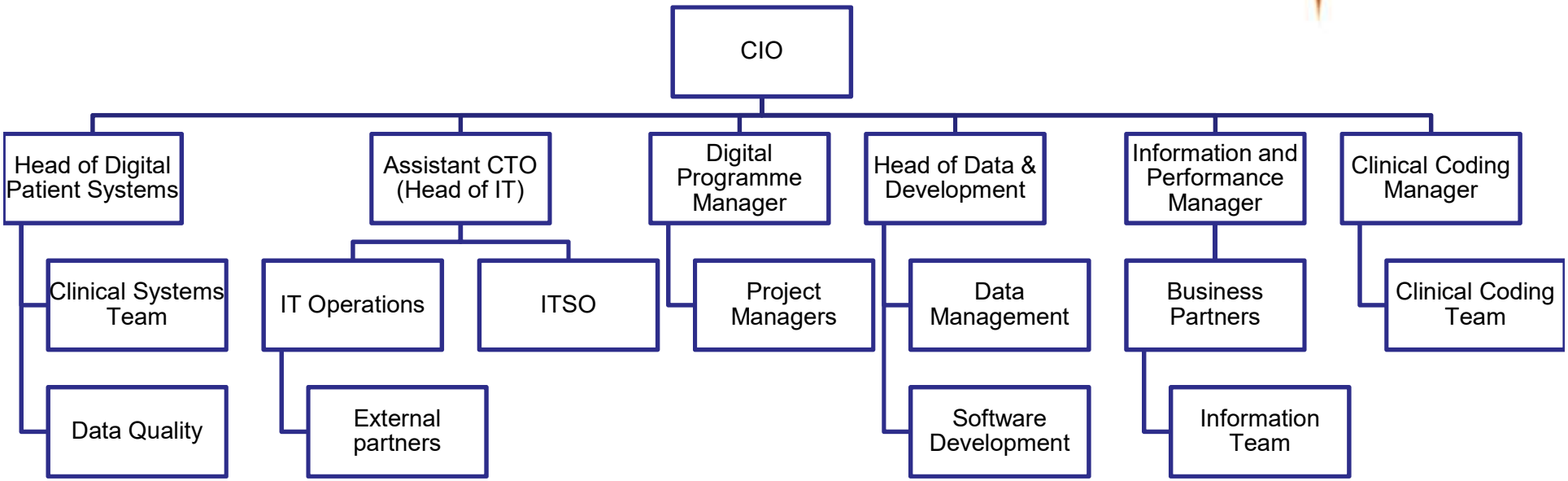
Part 5: Sign-off and approval

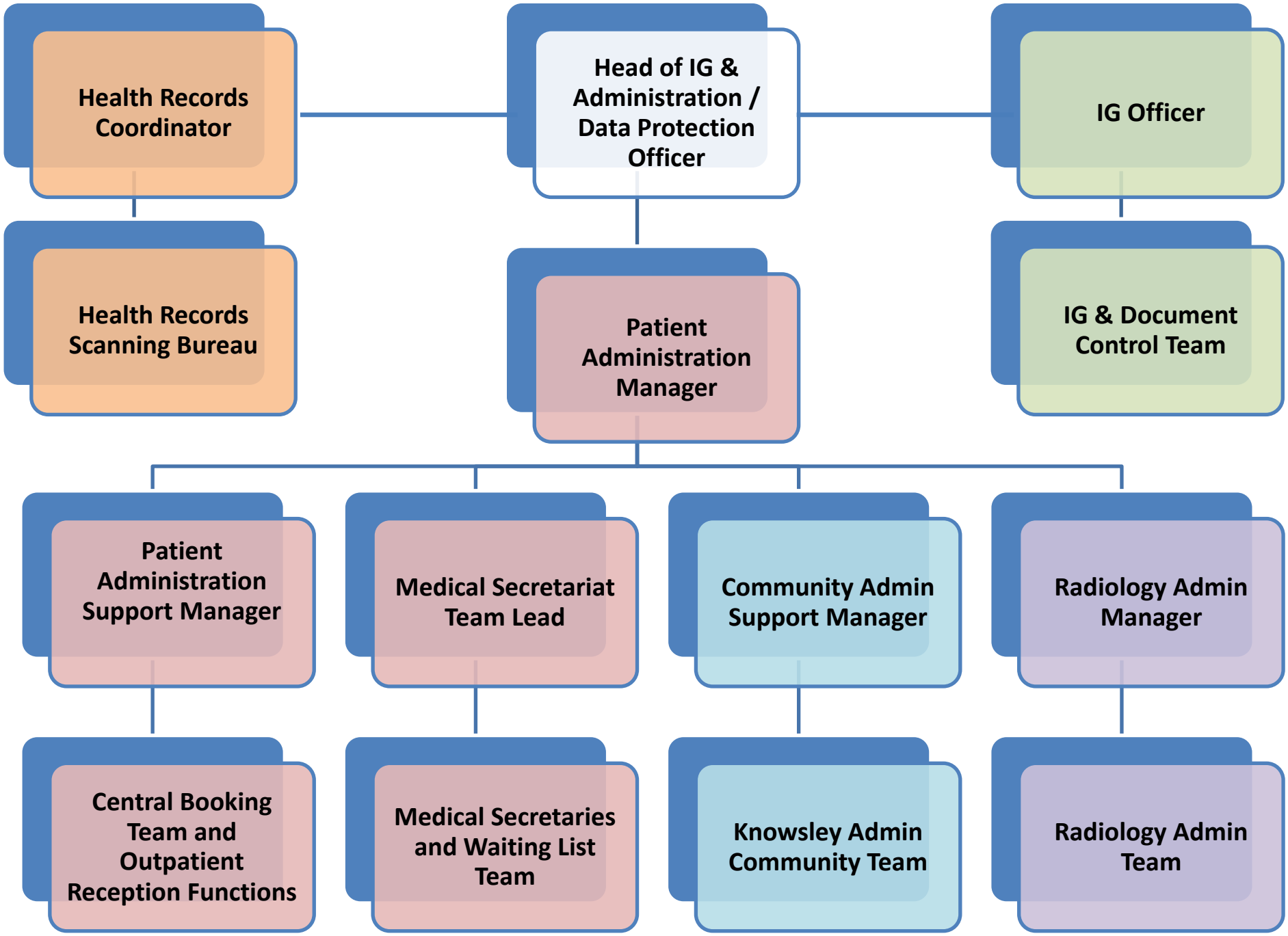
Operational sign-off Acceptance of the risks and mitigating actions		**SIRO approval**	
Name:		Name:	
Signature:		Signature:	

Date:		Date:	

Structure 2020

Liverpool Heart and Chest Hospital NHS
NHS Foundation Trust




Health Records Coordinator
Head of IG & Administration / Data Protection Officer
IG Officer
Health Records Scanning Bureau
Patient Administration Manager
IG & Document Control Team
Patient Administration Support Manager
Medical Secretariat Team Lead
Community Admin Support Manager
Radiology Admin Manager
Central Booking Team and Outpatient Reception Functions
Medical Secretaries and Waiting List Team
Knowsley Admin Community Team
Radiology Admin Team

JOB DESCRIPTION

Job Title:	Chief Information Officer
Band:	8d
Base	Liverpool Heart and Chest Hospital
Department / Portfolio	Digital Healthcare
Reports to:	Chief Financial Officer
Accountable to:	Chief Financial Officer

1. JOB PURPOSE

- Overall responsibility for the development and delivery of the Trusts digital strategy which supports the organisations long term vision and is compliant with all relevant regional and national policy.
- Professional leadership to the Digital Healthcare team which comprises IT, Clinical Systems, Business Intelligence, Clinical Coding and Data Quality functions.
- Accountable for the implementation of digital solutions and associated change programmes which enable business development and process changes to improve clinical quality, patient safety and reduce costs.
- Responsible for prioritising and planning the Trust's digital and informatics programme, ensuring that projects are delivered successfully on time and in budget.
- To lead the Business Informatics Transformation programme to support and develop high quality BI services which enable the Trust to continue to deliver outstanding care for its patients.
- To lead and champion the drive toward digital excellence and high standards of digital maturity.
- To deputise for the Chief Financial Officer on all matters within the scope of the role when required.

2. JOB SUMMARY

Reporting directly to the Chief Finance Officer the post holder will lead and direct the development and provision of all digital and business intelligence systems and services across the organisation.

Chief Information Officer is a specialist role which leads multi-skilled teams that are running and building secure and robust digital systems and processes to deliver and enhance patient care. The role also acts as a key enabler to improving business operations and driving value for money

from the Trust's investment in technology and business intelligence. This is a key post in supporting and leading the 'Digital Hospital' vision and agenda. The post holder will be the digital lead within LHCH, who will be responsible for all relevant digital modernisation strategies including, Five Year Forward View, Personalised Health and Care 2020, Sustainable Transformation Programmes, Local Digital Roadmaps and the Model Hospital.

This role will lead the entire digital and analytics agenda for the Trust, ensuring that LHCH maximises all potential opportunities provided from the implementation of new digital systems, software, analytics and ways of working. This post has a critical role to play in ensuring that the digital agenda is fully aligned with the key objectives of the Trust and enabling wider business and clinical transformation in order to deliver new ways of working and the realisation of benefits, both in terms of finance and quality.

The post holder will be required to lead a complex Business Information change management programme to develop high quality, effective and efficient processes which meet the changing needs of the organisation in the delivery of its vision.

This is a customer focused role that will support the Trusts leaders, clinicians and staff at all levels to ensure that the digital healthcare team provides a service that is responsive to the needs of the Trust. The post holder will be responsible for communicating highly complex information in relation to digital service developments and this will require the highest level of interpersonal skills in order to convey complex technical information in a way the wider organisation can understand and engage with.

The post holder will lead, develop and manage the Digital Healthcare Team, comprising of approx. 50 staff across IT, Clinical Systems, Business Intelligence, Clinical Coding, Information Governance & Security and Data Quality functions. He/she will decide on most effective use of all digital resources, evaluate service effectiveness and service performance, and make judgements on a wide range of highly complex service issues underpinning healthcare service delivery.

3. MAIN DUTIES AND RESPONSIBILITIES:

- **Strategy**
- Responsible for the development and delivery of the Trusts digital strategy which supports the organisations long term vision, supports service and cost improvement and is compliant with all relevant regional and national policy.
- Coordinate the production of medium and long terms plans which underpin the delivery of the strategy.
- Play a key role in shaping and supporting the Cheshire and Merseyside STP digital strategy through strong engagement and leadership across Trusts in North Mersey and the wider STP footprint.
- Champion the strategic value of effective information technology and business intelligence ensuring that the principles adopted will enhance the corporate objectives of the Trust and other organisations within the local health community.
- Scope, manage and work with the Digital Healthcare Committee and Capital Management Group to identify the financial resources required to deliver the digital healthcare strategy for the Trust and delivery projects on time and within budget. This will require development of 5 year resource and capital plans.
- Transfer expertise and knowledge as appropriate, throughout the team and Trust wide. This will include developing and delivering formal communication briefings and training to promote innovation and update on progress in key projects and objectives.

- Lead managerial, clinical and operational engagement across the Trust in developing and implementing a digital healthcare strategy.
- To forge positive working relationships, in order to support an effective approach to achieve the objectives of the Trust within the overall objectives of the NHS.
- Be a credible and respected leader, able to convince peers and effectively manage a large digital team (approx. 50 staff).
- Foster effective relationships with external partner agencies in health and social care as appropriate to ensure the effective delivery of clinically led digital initiatives.
- Maintain and review partnership working relationships with suppliers and sub-contractors and ensure that commercial relationships are managed and developed.
- Recruit and commission additional services as necessary, performance managing internal and external resources to deliver a range of tasks in a challenging environment.

- **Leadership**

- The post holder will lead, develop and manage the Digital Healthcare Team, comprising of approx. 50 staff across IT, Clinical Systems, Business Intelligence, Clinical Coding, Information Governance & Security and Data Quality functions.
- Work with the Chief Finance Officer to build a single integrated (Digital Healthcare) team from the current Digital Systems and Informatics teams.
- To provide professional leadership to the digital team though actively developing the team both as individuals and also as a cohesive and integrated team, engaging with national and regional development opportunities where appropiate (e.g. through ISD)
- Create a culture of engagement, feedback, collaboration and connection to purpose and context, ensuring the team has a clear vision and direction, and are clear in how their roles support the delivery of this vision.
- Build effective relationships with colleagues at all levels through open communication and constructive feedback. Be a trusted expert partner in the delivery of digital services to support clinical and operational Trust business.
- Ensure “digital users” across the organisation are appropriately trained to work digitally so the Trust maximizes the benefit of its investment.
- Develop and ensure that all digital stakeholder experience measures are reported and benchmarked and that appropriate KPIs are developed and monitored.
- Provide leadership for Information Asset Owners (IAOs) of the Organisation through effective networking structures, sharing of relevant experience, provision of training and creation of information risk reporting structures.
- Take the lead in the recruitment, retention, performance management and development of staff across the digital healthcare team and ensure that professional and governance standards are applied within the department. Ensure that all mandatory training is undertaken within the team.
- Develop the role of business partnering in relation to digital functions.
- Represent the Trust in terms of digital healthcare at local, Regional and National level. In particular, take an active role in the CIAG (or similar) and ISD developments and ensure the

Trust's position is taken into account in decision making on overall strategic, policy and procedural matters.

- **Planning and Organising**

- Lead the Digital Healthcare team to ensure the translation of strategies and policies into plans for implementation – clarifying outcomes, key milestones, objectives and a monitoring framework.
- Develop plans for the delivery of the digital healthcare strategy, including identifying interdependencies, managing risks, modelling the potential impacts on the wider organisation, determining resource requirements and building in contingency where necessary.
- To lead the Business Informatics Transformation programme to support and develop high quality BI services which enable the Trust to continue to deliver outstanding care for its patients.
- Accountable for the implementation of digital solutions and associated change programmes which enable business development and process changes to improve clinical quality, patient safety and reduce costs.
- Proactively mitigate risk across all activity, ensuring that risks are understood within the organisatsions wider risk management policy and that they are appropriately managed and mitigated where possible.
- Ensure that there are policies, processes and procedures in place for the organisation to ensure that all information is effectively recorded, managed, preserved, analysed and disseminated in accordance with best practice and in compliance with legal, statutory and ethical requirements.
- Deliver regular updates to the various Trust Committees to provide timely communication regarding the progress of digital projects and other deliverables. This will include Risk Management and Corporate Governance Committee, Executive Leadership Team and Digital Healthcare Committee amongst others.

- **Quality**

- To develop an effective data quality framework for key patient systems, including the development of effective data quality monitoring mechanisms and robust policies and procedures for clinical and administration staff.
- Working with the Information governance lead to ensure that the Trusts is compliant with GDPR requirements.

- **Financial and Contract Management**

- Responsible for all digitally related budgets (revenue budgets of approx. £4.2m per annum plus capital investment budgets as agreed), ensuring compliance with SFI's and obligations to CIP initiatives are met.
- Incorporate departmental objectives, quality plan, financial and equipment issues into business plans.
- Constantly strive for value for money and greater efficiency in the use of corporate finances and to ensure that they operate in recurrent financial balance year on year.

- Negotiate and manage suppliers to ensure the Trust obtains value for money from its digital investment.
- Work with operational managers to ensure delivery of financial and other benefits from digital developments.
- Ensure arrangements are in place for monitoring the effective delivery of key Service Level Agreements (SLA) between the Trust and its third party service providers.
- Ensure the Trust is ready to make applications and is successful in obtaining NHS external funding for digital working.

- **KEY WORKING RELATIONSHIPS AND COMMUNICATION**

Internal to the Trust	External to the Trust
• Chief Executive, Executive Directors, Non-Executive Directors, Associate Directors • Divisional Heads of Operations • Chief Clinical Information Officer & Associates • Chief Nursing Information Officer & Associates • Heads of Departments • Trust senior and junior consultants, medical and nursing staff	• Working across boundaries often as part of collaborative initiatives • Senior Managers within neighbouring hospitals • Working with other external partners i.e. universities, social care, commissioners, professional bodies, other organisations • Working with suppliers and vendors • Working with legal representation • Working with national guidance and compliance bodies e.g. ICO and HSCIC

- **GENERAL STATEMENTS**

6.1 Confidentiality
All employees must adhere to policies and procedures relating to Information Governance, Confidentiality and Information Security.

6.2 Risk Management
The Trust is committed to approaching the control of risks in a strategic and organised manner. The post holder must be aware of their individual responsibilities as detailed in the Trusts Risk Management, Health & Safety and Incident policies, and those under the Health and Safety at Work Act. This includes the reporting of any untoward incident, accident, potential or actual hazard identified.

6.3 Safeguarding
All staff are required to be familiar with the arrangements for safeguarding children, young people and vulnerable adults and support the organisation in promoting the welfare of children, young people and vulnerable adults.
Staff working directly with children, young people and vulnerable adults will have a responsibility to ensure safeguarding and promoting their welfare forms an integral part of their duties.
Staff who come into contact with children, vulnerable adults, parents and carers in the course of their work and/or have access to records will have responsibilities to safeguard and promote the welfare of children, young people and vulnerable adults.
Staff who come into contact in the course of their duties, with parents, carers or other significant adults or children, young people and vulnerable adults should always be mindful of safeguarding and promotion of the welfare of these individuals.

6.4 Health and Wellbeing
The Trust is a Health Promoting Hospital. The Trust expects that when you are presented with opportunities to improve the lifestyle of our patients you seek help from appropriately trained clinical staff to ensure patients are supported and assisted in making the necessary lifestyle changes. This is in accordance with best practice as described in the DoH white paper "Choosing Health – Making Healthy Choices Easier".

6.5 Equal Opportunities

The Liverpool Heart & Chest Hospital NHS Foundation Trust is committed to achieving equal opportunities. All employees are expected to observe this policy in relation to the public and fellow employees.

All staff are expected to adhere to, and act in accordance with, the values & behaviours of the Trust.

This document is intended to be used as a guide to the general scope of duties involved in this post. It is not exhaustive and should not therefore be used as a rigid specification. It will be kept under review and amended as required in consultation with the post holder.

Signed (Employee)……..... Date……

Signed (Manager)……..... Date……

LIVERPOOL HEART & CHEST HOSPITAL NHS FOUNDATION TRUST

JOB DESCRIPTION

POST:	**Data Protection Officer**
BANDING:	**Assigned to Senior Management Level**
ACCOUNTABLE TO:	**Trust Board Lead - GDPR**
RESPONSIBLE FOR:	**Data Protection Compliance and Assurance**

JOB SUMMARY

The Purpose of the Data Protection Officer (DPO) is to provide the organisation independent risk-based advice to support its decision-making in the appropriateness of processing Personal and Special Categories of Data within the Principles and Data Subject Rights laid down in the General Data Protection Regulation (GDPR). This role is legally required in line with Articles 37, 38 and 39.

PRINCIPAL ACCOUNTABILITIES

- Inform and advise the Data Controller or Data Processor and the employees who carry out processing of their Data Protection obligations.
- Monitor Data Protection compliance.
- Assign responsibilities, awareness-raising and training of staff involved in processing operations.
- Undertake internal audits of Data Protection.
- Provide advice on the need and completion of Data Protection Impact Assessments, including approval sign off.
- Cooperate with the ICO and act as the contact point for any issues relating to processing
- Undertake or advise on the potential risk of processing activities.

The above will include, but is not limited to:

- Leading from the front in promoting an appropriate Data Protection culture within the organisation.
- Setting organisational trigger-points for mandatory input from the DPO.
- Close liaison with senior clinical and non-clinical colleagues to enable and support both operational and strategic decision-making.
- Management of a governance structure to record Data Protection decisions made by the organisation.
- Provision of advice on complex Data Protection issues, such as Subject Access Requests, procurement decisions, Information / Cyber Security and Information Sharing.
- Sign-off of regulatory requirements, e.g. Information Governance Toolkit submissions.
- Maintaining ongoing personal development and knowledge of Data Protection law, issues and developments.

Under GDPR, Data Protection Officers have rights in addition to their responsibilities. The Data Protection Officer:

- May insist upon resources to fulfil their job functions and for their own ongoing training.
- Must have access to the company's Data Processing personnel and operations.
- Have significant independence in the performance of their roles.
- Have a reporting line 'to the highest management level' of the organisation.

PERSON SPECIFICATION, SKILLS AND KNOWLEDGE

Demonstrable expert knowledge of Data Protection law and practices, gained by formal qualification and / or experience.

In-depth knowledge and practical experience of the NHS.

Confidence, although employed by the organisation, to act “as if” independent, especially when liaising with senior colleagues and Trust Board.

The equivalent seniority of ’Senior Manager’ Band 8 or above.

Created by:	**Head of Data Protection & Administration**	**Dated**	**December 2017**

LIVERPOOL HEART & CHEST HOSPITAL NHS FOUNDATION TRUST

JOB DESCRIPTION

POST:	**Head of Information Governance & Administration**
BANDING:	**8b**
ACCOUNTABLE TO:	**Deputy Director of Nursing and Quality**
RESPONSIBLE FOR:	**- Information Governance** **- Health Records Service** **- Patient Access and Administration Services (Access and Booking Team, Medical Secretariat, Waiting List Team, 18 Week Validation Team, Outpatient Reception)**

JOB SUMMARY

1. Strategic management and leadership for Information Governance, Health Records and Patient Administration services, ensuring appropriate assurance and accountability frameworks are implemented.

2. Receive, assimilate, analyse and present complex data / information and processes in areas of responsibility to ensure compliance with national standards and legislation including Data Protection, Freedom of Information, Information Governance, Health Records Management, Patient Access and Administration, ERS, and RTT.

3. Develop business cases and service planning in all areas of responsibility to support service integration, standardisation, introduction of digital technologies, and financial efficiency to support wider trust strategic objectives.

4. Assigned role as Data Protection Officer to implement and fulfil the statutory functions in line with the requirements outlined in the General Data Protection Regulation (GDPR) - refer to Data Protection Officer Job Description.

PRINCIPAL ACCOUNTABILITIES

1. Development and implementation of strategies, policies and procedures within areas of responsibility.

2. Requirement to interpret national policy and legislation within area of remit to be implemented at LHCH.

3. Responsible for the implementation and monitoring of the Access Policy to support delivery of national waiting times ensuring key functions and processes provide a robust approach including referral management, waiting lists and booking processes.

4. Senior Trust Lead for Data Protection and Freedom of Information.

5. Analyse, interpret and present data to highlight issues and risks ensuring mitigating action is taken.

6. Data Protection Officer under GDPR responsible for fulfilling statutory functions, providing leadership, challenge and support to achieve organisational compliance whilst maintaining an impartial and independent approach.

7. Support the Senior Information Risk Owner (SIRO) and Caldicott Guardian in discharge of their duties, providing professional guidance and expertise.

8. Ensure compliance with statutory returns / evidence as required relating to areas of responsibility, including performance assessment frameworks and national mandates e.g. Data Protection & Security Toolkit, CQUIN, NHS Digital, ICO etc.

9. Work in conjunction with clinicians and clinical divisions to develop enhancements to services and contribute to long term strategic planning.

10. Develop relationships and collaborative working with external partners such as NHS Digital, NHS England, CCG's, primary care etc.

11. Implement monitoring and audit processes to assess compliance with policies and procedures within areas of responsibility.

12. Collate and analyse reports and statistics related to referral management, 18 weeks RTT, waiting lists, outpatient activity, Information Governance and Health Records, to identify trends or deficiencies to drive further improvement.

13. Membership and attendance at relevant Trust committees, working groups and meetings, where required to act as Chair or participate in accordance with relevant terms of reference.

14. Lead change across a number of agendas and projects to improve effectiveness and efficiency, implementing key changes to services in areas of responsibility.

15. Trust representative on various organisational, local and national groups in determining implementation of national or local policy.

16. Involved with contract tender processes for the procurement of goods, services or contracts within area of responsibility. Act as lead for relevant contracts established and ensure monitoring compliance with service provider to deliver a quality, effective and cost effective services.

17. Monitor activity levels; identify cost pressures, service development opportunities and operational performance of structures, ensuring proactive management of issues escalating if required.

18. Contribute to the Trust annual business planning process, ensuring adequate resource is available to support demand in areas of responsibility.

19. Work with high levels of autonomy and independence to make decisions in areas of responsibility, ensuring any impacts of changes are considered to minimise risk.

20. Support and propose developments to IT systems to further enhance quality, safety and operational efficiency, working with system suppliers and information asset owners to achieve optimal outcomes.

21. Encourage a continuous improvement quality improvement approach in the development and implementation of processes, ensuring patient care is the key focus.

22. Be involved with partner organisations in strategic and operational changes to local services and collaboration.

MANAGERIAL/LEADERSHIP

1. Provide professional management, leadership and expert advice within areas of responsibility.

2. Develop strategic and performance objectives within all areas of responsibility, to provide assurance on successful implementation, compliance and performance.

3. Support a culture where individuals feel able to report incidents, concerns or opportunities for improvement, and ensure learning takes place from all incidents and complaints.

4. Responsibility for human resource management, recruitment, application of human resource policies as required.

5. Determine, drive and lead schemes of work, identifying interdependencies across departments / functions, potential impacts on wider organisation, resource requirements, and operational management support.

6. Accountable for financial budgets within areas of responsibility, ensuring projects, services and resources are managed in a cost efficient manner, monitoring expenditure against target.

7. Provide leadership and support development of staff within responsible functions to ensure sufficient knowledge, skills and expertise are available to deliver operational objectives with high levels of competence and confidence.

8. Provide leadership underpinned by strong values of equality, diversity and openness, effectively building and maintaining relationships with staff and key stakeholders internal and external to the Trust.

9. Demonstrate and encourage leadership in everyday practice to support innovation, development, delegation, organisation and prioritisation to support safe and effective delivery of services, including excellent patient and service user experience.

10. Ensure risks, issues and complaints are investigated and managed in accordance with Trust policy, ensuring feedback and learning is promoted to constructively manage improvements.

11. Develop dashboards and compliance monitoring framework to ensure visibility of productivity, quality and compliance, allowing for meaningful feedback to functions to drive improvement.

12. Ensure team objectives are clearly defined with appropriate levels of accountability and responsibility assigned within the structure.

13. Act professionally and calmly, using tact and diplomacy, to a range of difficult or emotional situations with staff and service users.

14. Ability to diagnose resistance to change, to change attitudes and motivate individuals and groups.

15. Use process mapping tools to improve systems and processes and demonstrate through measurable means how improvements have added value or reduced cost.

ORGANISATIONAL

1. Communicate and provide complex information to a wide range of internal and external stakeholder.

2. Present complex information about projects, initiatives, systems and processes to a wide range of stakeholders.

3. Support collaborative working across internal functions within the Trust and external organisations.

PROFESSIONAL

1. Undertake required professional certification / accreditation to maintain expert knowledge and understanding within areas of responsibility, and maintain a detailed working knowledge of standards required to be implemented.

GENERAL STATEMENTS

CONFIDENTIALITY

All employees must adhere to policies and procedures relating to Information Governance, Confidentiality and Information Security.

RISK MANAGEMENT

The Trust is committed to approaching the control of risks in a strategic and organised manner.

The postholder must be aware of their individual responsibilities as detailed in the Trusts Risk Management, Health & Safety and Incident policies, and those under the Health and Safety at Work Act. This includes the reporting of any untoward incident, accident, potential or actual hazard identified.

SAFEGUARDING

All staff are required to be familiar with the arrangements for safeguarding children, young people and vulnerable adults and support the organisation in promoting the welfare of children, young people and vulnerable adults.

Staff working directly with children, young people and vulnerable adults will have a responsibility to ensure safeguarding and promoting their welfare forms an integral part of their duties.

Staff who come into contact with children, vulnerable adults, parents and carers in the course of their work and/or have access to records will have responsibilities to safeguard and promote the welfare of children, young people and vulnerable adults.

Staff who come into contact in the course of their duties, with parents, carers or other significant adults or children, young people and vulnerable adults should always be mindful of safeguarding and promotion of the welfare of these individuals.

INFECTION CONTROL

In accordance with the Health and Social Care Act 2008, it is the responsibility of every member of staff to participate in the prevention and control of infection within the capacity of their role. In order to maintain high standards of infection and prevention control all staff are expected to comply with the relevant Trust policies, procedures and guidelines and report any concerns to their manager or to the infection prevention team.

HEALTH AND WELLBEING

The Trust is a Health Promoting Hospital. The Trust expects that when you are presented with opportunities to improve the lifestyle of our patients you seek help from appropriately trained clinical staff to ensure patients are supported and assisted in making the necessary lifestyle changes. This is in accordance with best practice as described in the DoH white paper "Choosing Health – Making Healthy Choices Easier".

EQUAL OPPORTUNITIES

The Liverpool Heart & Chest Hospital NHS Foundation Trust is committed to achieving equal opportunities. All employees are expected to observe this policy in relation to the public and fellow employees.

All staff are expected to adhere to, and act in accordance with, the values & behaviours of the Trust.

This document is intended to be used as a guide to the general scope of duties involved in this post. It is not exhaustive and should not therefore be used as a rigid specification. It will be kept under review and amended as required in consultation with the postholder.

Created by:	**Head of Data Protection & Administration**	**Dated**	**December 2017**

Liverpool Heart and Chest Hospital NHS
NHS Foundation Trust

JOB TITLE: **Senior Information Risk Owner**

RESPONSIBLE TO: **Chief Executive**

JOB SUMMARY

The position of Senior Information Risk Owner (SIRO) will be the responsibility of the assigned board level director who will take overall ownership of the Organisation's information security and risk policies, act as champion for information risk on the board and provide written advice to the Accounting Officer on the content of the Organisation's Statement of Internal Control in regard to information risk.

The SIRO is expected to understand how the strategic business goals of the Organisation and how other NHS Organisations' business goals may be impacted by information risks, and how those risks may be managed.

The SIRO will implement and lead the Trust's information governance agenda and information risk management processes within the organisation and will advise the board on the effectiveness of information security risk management across the Trust.

The SIRO shall receive training as necessary to ensure they remain effective in their role as Senior Information Risk Officer.

KEY RELATIONSHIPS

Within the Organisation:

- Chief Executive and other Board members
- Caldicott Guardian
- Risk Lead
- Head of Information Governance & Administration
- Chief Information Officer
- IT Security Officer
- Head of IT

Regularly has contact with:

- Chief Executive, other Senior Information Risk Owners, Caldicott Guardians and Information Governance Leads of Department of Health and other NHS Organisations.

KEY RESPONSIBILITIES

1. **Policy and process**

- Oversee the development of the Trust's Information Risk Policy. This should include a Strategy for implementing the policy within the existing Information

Governance Assurance Framework and be compliant with NHS IG policy, standards and methods.

- Take ownership of the assessment processes for information risk, including prioritisation of risks and review of the annual information risk assessment to support and inform the Statement of Internal Control.
- Ensure that the Board are kept up to date and briefed on all information risk issues affecting the organisation and its business partners.
- Review and agree actions in respect of identified information risks.
- Ensure that the Organisation's approach to information risk is effective in terms of resource, commitment and execution, being appropriately communicated to all staff.
- Alongside the Head of Information Services and Risk Manager provide a focal point for the escalation, resolution and/or discussion of information risk issues.
- Ensure that an effective infrastructure is in place to support the role by developing a simple information governance structure, with clear lines of information asset ownership and reporting with well-defined roles and responsibilities.
- Ensure robust policies and processes are in place for the management of the Registration Authority function.

2. **Incident Management**

- Ensure that identified information threats and vulnerabilities are followed up for risk mitigation, and that perceived or actual information incidents are managed in accordance with NHS IG requirements and Trust policy.
- To ensure that there are effective mechanisms in place for reporting and managing Serious Untoward Incidents (SUIs) relating to the information of the organisation. These mechanisms should accommodate technical, operational or procedural improvements arising from lessons learnt.

3. **Leadership**

- Collaboratively provide leadership and guidance for Information Asset Owners (IAOs) of the organisation through effective communication, sharing of relevant experience, provision of training and creation of information risk reporting structures.
- Advise the Board on the level of Information Risk Management performance within the Organisation, including potential cost reductions and process improvements arising etc

TRAINING

The SIRO will be required to undertake information risk management training at least annually to be able to demonstrate their skills and capabilities are up to date and relevant to the needs of the organisation.

Cyber Security and Information Governance Group

Terms of Reference

For completion by Author			
Author(s) Name and Title:	P Fagan (IT Programme Manager) / W Taylor (IG & Health Records Manager)		
Scope:	Trust Wide	Classification:	Non-Clinical
Version Number:	2.0	Review Date:	September 2021
Replaces:	1.4		
To be read in conjunction with the following documents:	Information Security Management System Information Governance Policy Information Governance Strategy		
Document for public display:	YES		
Executive Lead	Karen Edge		

For completion by Approving Committee			
Equality Impact Analysis Completed:		N/A	
Endorsement Completed:	N/A	Record of Changes	No
Authorised by:	Dr Raphael Perry on behalf of Digital healthcare Committee	Authorisation date:	01/06/2020

For completion by Document Control					
Unique ID No:	TOR/DH/01(17)	Issue Status:	Approved	Issue Date:	08/06/2020
After this document is withdrawn from use it must be kept in archive for the lifetime of the Trust, plus 6 years.					
Archive:	Document Control		Date Added to Archive:		
Officer responsible for Archive:		IG and Document Control Facilitator			

Contents

1. Constitution and Remit

The Cyber Security & Information Governance Group (CSIGAG) is established as a sub group of Digital Healthcare Committee of Liverpool Heart and Chest Hospital NHS Trust to provide operational support, preparedness and direction to address and reduce cyber risk and improve the Trust's cyber defences. It shall act as a source of knowledge and expertise, manage NHS Digital CareCERT alerts, will oversee and monitor the Cyber Security Action Plan, receive progress reports on information governance, with recommendations, progress and assurance reported to Digital Healthcare Committee.

2. Authority

The CSIGAG has delegated authority via the Digital Healthcare Committee to lead on all matters relating to Information Governance, cyber security and management of risk in relation to cyber security related issues.

3. Objectives and Duties

The purpose of the CSIGAG is to;

- Promote and increase awareness around cyber security issues and initiatives to the Board of Directors and staff
- Develop and collaborate regarding cyber security best practice to ensure the Trust's IT infrastructure and data is protected
- Oversee and monitor completion of the Information Asset Register and System Level Security Policies
- Develop the Trust's cyber incident response, categorization and reporting procedures for IM&T Programme Board approval
- Oversee and monitor the cyber security action plan
- Develop a log of, review and manage the response to any NHS Digital CareCERT and other cyber security alerts
- Act as the expert advisory forum on cyber security related matters
- Share information and lessons learned regarding cyber security and the Trust's ISMS
- Discuss information and awareness around emerging technology, vulnerabilities and risks
- Support development of Information Governance policies, Data Security and Protection Toolkit action plans, and Caldicott associated issues
- Support implementation of and monitor information governance standards, in particular progress against the IG Strategy

4. Integration

n/a

5. Membership

The CSIGAG will comprise of the following:

- Chief Information Officer (Chair)
- Information Governance & Health Records Manager / Data Protection Officer (Deputy Chair)
- Chief Finance Officer (SIRO)
- Head of IT
- Medical Devices Manager
- IT Security Officer
- PACS/RIS Manager / Chief Safety Officer
- IG Officer
- Client Representative (IM)
- IT Technical Specialist (IM)
- IT Operations Coordinator (IM)

Other individuals may be co-opted or requested to attend meetings as required to present papers, support work plans or provide assurance.

6. Attendance

Members are required to attend 70% of the meetings.

7. Quorum and Frequency

The Quorum of the CSIGAG shall be 50% of its membership.

Meetings should be focused (1-2 hours) but give members the opportunity to raise any other issues that are not covered by the formal agenda. The group will meet quarterly unless otherwise required.

8. Reporting

The Group will report to the Digital Healthcare Committee via hot topics.

9. Conduct of Committee Meetings

The Chair of the committee will ensure that the appropriate processes are followed:

- Action Log
- Matters arising
- CareCERT log
- Incidents
- Progress against Information Asset Register & System Level Security Policies
- Progress against cyber security action plan

- Progress against data protection toolkit action plan
- Information Governance Progress Report
- Risks

10. Other Matters

n/a

Risk Management, Corporate Governance & Health & Safety Committee

Terms of Reference

For completion by Author			
Author(s) Name and Title:	Dr Margarita Perez-Casal, Director of Research & Innovation; Chief Risk Officer		
Scope:	Trust Wide	Classification:	Terms of Reference
Version Number:	1.2	Review Date:	17 November 2020
Replaces:	v1.1		
To be read in conjunction with the following documents:	Governance Manual Annual Work Schedule Board Assurance Framework Risk Management Policy		
Document for public display:	Yes		
Executive Lead	Dr Margarita Perez-Casal, Director of Research & Innovation; Chief Risk Officer		

For completion by Approving Committee			
Equality Impact Analysis Completed:			
Endorsement Completed:		Record of Changes	
Authorised by:	Board of Directors	Authorisation date:	17 December 2019

For completion by Document Control					
Unique ID No:	TOR/T20DC022	Issue Status	Approved	Issue Date:	28/02/2020
After this document is withdrawn from use it must be kept in archive for the lifetime of the Trust, plus 6 years.					
Archive:	Document Control	Date Added to Archive:			

Contents

1. Constitution and Remit

This committee is established as a reporting Committee to the Operational Board of Liverpool Heart and Chest Hospital NHS Foundation Trust.

2. Authority

The Risk Management and Corporate Governance Committee (RMCG) is authorised to investigate any activities within the scope of its terms of reference and obtain any information required from relevant parties to facilitate its understanding of the issues.

With respect to Estates services, and where appropriate the Committee will consider the Broadgreen site in totality where this will have an impact on the way the Trust delivers its services.

3. Objectives & Duties

The RMCG will run in two parts:

2.1 Part A will cover Risk Management and Corporate Governance (excluding Health and Safety)
2.2 Part B will focus on Health and Safety

The committee will deliver the following objectives:

Part A

3.1 Risk Management

a) To oversee organisation-wide (enterprise) risk management ensuring equal emphasis on future risk exposure as well as current operational risk exposure.
b) To provide leadership to ensure risk is identified and managed proactively in accordance with the Board's risk appetite.
c) To assure the adequacy of risk treatment plans.
d) To champion and promote highly-effective risk management practices and ensure that the risk management process and culture are embedded throughout the Trust.
e) To maximise the delivery of objectives through an effective control system.
f) Strive to keep risk under prudent control at all times and minimise over-exposure to risk.
g) To improve the standard of decision making on risk management.
h) Systematically review, scrutinise and challenge those risks with a score above 12 across Divisions and Corporate Departments ensuring the optimum strategy is adopted for managing each key risk; controls are present and effective and action plans are robust for those risks which remain intolerant. Divisions and Departments will be asked to present their high risks (score ≥12) at each meeting with clear mitigations and controls put in place.
i) Satisfy itself and the Board that the structures, processes and responsibilities for identifying and managing key risks to patients, staff and the organisation are adequate.

j) Monitor, evaluate and scrutinise all risks placed on the risk register with a residual risk rating of 10 or above and escalate to the Board those that pose a significant threat to the operations, resources or reputation of the Trust (scores >=15).

k) Review and approve the Trust's Risk Management policies and procedures.

l) Review the capacity to handle risk ensuring all requirements are met for the Chief Executive to sign the Annual Governance or other relevant public disclosure statements.

m) Review trends in adverse event reports on a six monthly basis (including incidents, complaints and claims) and take decisions regarding appropriate steps to reduce re-occurrence.

n) Work closely with all relevant committees and operational groups, in particular - Integrated Performance; Quality; Audit Committee and People Committee

o) The Chair of the Committee shall attend an annual meeting with the Audit Committee to ensure appropriateness of risk management structures. In addition, to make recommendations concerning the annual programme of Internal Audit work, to the extent that it applies to matters that fall within these Terms of Reference.

p) Ensure that all risks are managed in line with the Trust's Risk Management Policy.

q) Review Risk Management effectiveness from:

- Performance against policy KPI's
- Central Alert System responsiveness
- Risk Management audits

3.1 Estates

a) Meets all recognised standards, including equality and diversity issues by presenting external reviews and internal audit information that benchmarks the Estate operation against best practice.

b) Monitor Estates KPI's.

3.2 Business Continuity and Emergency Planning

a) Ensure that the Trust has a robust plan in place to ensure business continuity in the event of a major incident.

b) Ensure that the Trust has an effective Emergency Planning process that supports the preparedness for and reaction to such an event, to include a robust disaster recovery plan.

3.3 Corporate Governance

a) Review and guide the development and implementation of corporate governance systems and processes.

b) Approve the establishment, work plans, duration and effectiveness of sub-committees and working groups.

c) To receive relevant measures of performance at each meeting and review and manage delivery.

d) Report to the Operational Board areas classified as major concern using our risk

e) scoring methodology.

f) Review of Serious Untoward Incidents (SUI's) and reporting to external agencies

g) (e.g. STEIS).

h) Develop a culture of effective risk management and corporate governance across the Trust.

Part B

3.2 Health and Safety

a) Approve the Trust's Health and Safety Policy and monitor adherence to it and take assurance that the Trust operates in a way that meets all regulatory requirements.
b) Continue to improve the H&S culture for the Trust by effective management of H&S risks throughout the Trust and the monitoring of Ward / Department H & S annual assessments.
c) To review data on incidents to staff, patients and visitors, identifying trends and ensuring appropriate action is taken.
d) To consider reports and other information provided by the Health and Safety Executive and other external bodies and recommend appropriate action.
e) Monitor the Trust's performance in relation to H&S KPIs.
f) To monitor compliance of H&S policies, fire safety and produce an annual report.
g) To review, consult and ratify policies pertaining to H&S.

4. Chairmanship

The Director of Research & Innovation shall be the Chairperson of the Risk Management & corporate Governance Committee. In the absence of the Director of Research & Innovation the Chief Operating Officer will chair the meeting.

Part A Membership:

Risk Management & Corporate Governance Committee:

Director of Research & Innovation (Chair)
Chief Operating Officer (Deputy Chair)
Divisional Head of Operations-Surgery (or HoN)
Head of Estates
Head of Human Resources or Head of Education
Chief Information Officer
Deputy Director of Finance
Chief Pharmacist
Risk & Safety Lead
Medical Engineering Manager
Patient Access & Administration Manager (or representative)
Other Heads of Corporate Departments (by invitation)

Part B Membership:

Health & Safety Committee:

Director of Research & Innovation (Chair)
Chief Pharmacist (Deputy Chair)
Divisional Head of Operations-Surgery (or HoN)
Risk & Safety Lead
Head of Estates
Head of Human Resources or Head of Education
Occupational Health Advisor
Infection Prevention and Control Nurse
Radiology Manager
Manual Handling Co-Ordinator
Trade Union, Health and Safety Representative (s)
Security Manager
Support Services Manager
Community Services Manager

Head of Nursing – Surgery

5. Quorum & Frequency

In order for decisions taken by the Chair or Deputy Chair and other members to be valid the meeting must be quorate. A quorum shall be the Chair (or deputy) and not less than three members. Each member shall be entitled to the right of one vote. Any resolution of the Committee shall require a simple majority of those present and voting.

In the event of an equality of votes the Chairperson shall have the casting vote.

The committee will meet every two months.

6. Organisation

The Committees are serviced by the Director of Research & Innovation who shall prepare the agenda and maintain a rolling programme of work for the Committee.

7. Attendance

Members are expected to attend at least 5 of the 6 meetings held each year but should aim to attend all scheduled meetings. Where they are unable to attend, they should send their designated nominated deputy.

8. Review

Terms of reference are reviewed annually or in the light of changes in practice or national/local guidance. The Committees will review annually their own performance, including the extent to which it has operated in satisfaction of its terms of reference, and in particular compliance with reporting arrangements to the Operations Board and monitoring thereof.

9. Reporting

The Risk Management & Corporate Governance Committee will report to the Operational Board assurances from each meeting in addition to an annual report.
The Risk Management & Corporate Governance Committee will receive an annual report and concerns/risks following each meeting from the following sub-committees:

- Health and Safety (Chair – Chief Operating Officer quarterly)
- Emergency Planning Group (Chair – Risk, Safety & Emergency Planning Lead; quarterly)

10. Conduct of Committee Meetings

The Chair of the committees will ensure that the appropriate processes are followed:

Part A:

- Review of Minutes from the previous meeting
- Action log
- Declarations of Interest
- Review of Risks scoring ≥12
- Business Continuity & Emergency Planning
- Estates

- Corporate Governance
- Date of next meeting

Part B:

- Review of Minutes from the previous meeting
- Action Log
- Declarations of Interest
- Occupational Health report
- RIDDOR incidents
- Estates and Fire safety report
- Security report
- Union H&S Representative report
- Date of next meeting

The agenda and supporting papers will be sent out to committee members five working days prior to the committee, unless authorised by the Chair for exceptional circumstances.

Authors of papers are expected to meet the set timeline from the work plan agreed by the committee.

Authors of papers presented must use the required template and indicate whether the paper is for decision by the committee, for discussion, for information or for approval.

Presenters of papers can expect all committee members to have read the papers and should keep a summary that outlines the purpose of their paper/report and key issues. Committee members may question the presenter.