Working together for Patients
Working together with Compassion
Working together as One Team
Working together Always Improving

NHS
Portsmouth Hospitals
NHS Trust

CONFIDENTIALITY AND DATA PROTECTION POLICY

Version	2
Name of responsible (ratifying) committee	Data Protection and Data Quality Committee
Date ratified	4 March 2020
Document Manager (job title)	Head of Information Governance and Data Protection Officer
Date issued	26 March 2020
Review date	03 March 2023
Electronic location	Management Policies
Related Procedural Documents	Data Quality Policy, Information Risk Policy, Personal Records-Access to Personal Records (Employee & Patient), Pseudonymisation Policy, Records Management Policy, Records Retention, Disposal and Destruction Policy, Secure Handling of Personal Information Policy, IT Security Policy
Key Words (to aid with searching)	Caldicott Principles, Caldicott Guardian, Confidentiality, Data Protection, GDPR, DPIA

Version Tracking

Version	Date Ratified	Brief Summary of Changes	Author
1	04/03/2019	New Document to replace Data Protection Policy and Confidentiality: Code of Conduct Policy	E Armour
2	04/03/2020	General policy formatting, new policy link added, 5.5 new paragraph added, item 4 - new definition added on patient confidentiality, item 4 – new definition added on breaches	C Froggatt

CONTENTS

QUICK REFERENCE GUIDE

The Trust has a legal obligation to comply with all appropriate legislation in respect of data, information and information security. It also has a duty to comply with guidance issued by the Department of Health (DH), the Information Commissioner's Office (ICO), the Care Quality Commission (CQC) and other advisory groups to the NHS and guidance issued by professional bodies.

The Trust is a public authority which collects and processes vast quantities of personal and special category data. As such we are required to abide by all relevant legislation pertaining to Data Protection and Confidentiality. The main legislation governing Data Protection are the GDPR (2016) and the DPA (2018) both of which have recently been enacted.

Health information which is collected from patients in confidence attracts the common law duty of confidentiality until it has been anonymized. This legal duty prohibits information use and disclosure without consent – effectively providing individuals with a degree of control over who sees information they provide in confidence. This duty can only be overridden if there is a statutory requirement, a court order, or if there is a robust public interest justification

The responsibility to withhold or disclose information without the data subject's consent lies with the senior manager or senior clinician involved at the time and cannot be delegated.

An individual requesting access to their health records may be refused access to parts of the information if an appropriate clinician deems exposure to that information could cause physical or mental harm to the data subject or a third party.

All project based research within the Trust must comply with the Data Protection & Caldicott Guardian Principles as set out within this Policy, be registered by the Research and Development Department and undergo review through the NHS Health Research Authority (HRA) approval process

To enable the Trust to address the privacy concerns and risks, the GDPR requires a Data Protection Impact Assessment (DPIA) be completed, and signed off by the Data Protection Officer and/or the DPDQ Committee.

The Trust is required to complete an annual review of Information Governance compliance by completing the on-line NHS Digital Data Security and Protection Toolkit.

The Trust must use appropriate technical and organizational measures, to ensure that personal data is processed in a manner to ensure the appropriate security of the data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage.

The CQC's well led inspection framework will include the importance of meeting the data security standards set out by the National Data Guardian.

1. INTRODUCTION

The Trust holds and manages a great deal of personal and confidential information relating to patients, service users and carers, the public and employees of the NHS. Data protection laws exist to strike a balance between the rights of individuals to privacy and the ability of organisations to use data for legitimate business purposes.

The Trust has a legal obligation to comply with all appropriate legislation in respect of data, information and information security. It also has a duty to comply with guidance issued by the Department of Health (DH), the Information Commissioner's Office (ICO), the Care Quality Commission (CQC) and other advisory groups to the NHS and guidance issued by professional bodies.

All legislation relevant to an individual's right of confidence and the ways in which that can be achieved and maintained, is paramount to the Trust. Penalties could be imposed upon the Trust, and/or Trust employees for non-compliance with relevant legislation and NHS guidance.

2. PURPOSE

This document describes Portsmouth Hospitals NHS Trust's (the Trust) policy on the Caldicott Guardian principles, the common law duty of Confidentiality and the Data Protection legislation. It describes the responsibilities of each employee with regard to safeguarding patient's, staff and the Trust's confidential information held both manually (not electronic, in a structured filing system) and electronic (computer). This policy aims to detail how the Trust meets its legal obligations and NHS requirements concerning confidentiality and data security standards.

3. SCOPE

This policy applies to all workers of the Trust to include:

- Permanent and fixed term contract employees, seconded employees
- Bank, agency and locum personnel
- Students, volunteers, apprentices
- Non-Executive Directors
- Researchers working within the Trust
- External contractors
- Employees of Engie – the Trust's PFI partner

'In the event of an infection outbreak, flu pandemic or major incident, the Trust recognises that it may not be possible to adhere to all aspects of this document. In such circumstances, staff should take advice from their manager and all possible action must be taken to maintain ongoing patient and staff safety'

4. DEFINITIONS

Confidentiality: Is the right of an individual to have personal, identifiable medical information kept private. Such information should be available only the physician on records and other care personnnel as necessary. The "Confidentiality: NHS Code of Practice" sets out what health and care organisations have to do to meet their responsibilities around confidentiality and patients consent to use their health records. It is based on legal requirements and best practice.

Data: Information which-

- is being processed by means of equipment operating automatically in response to instructions given for that purpose
- is recorded with the intention that it should be processed by means of such equipment
- is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system or
- does not fall within the above paragraph but forms part of an accessible record

Data Breach: A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data. A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

Data Controller: The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Data Flow: A continuing or repeated flow of information which takes place between individuals or organisations and includes personal data.

Data Processor: A natural or legal person, public authority, agency or other body which processes the data on behalf of the data controller.

Data Subject: An identified or identifiable natural living person to whom personal data relates

Direct Care: The provision of clinical services to a patient that require some degree of interaction between the patient and the health care provider.

Duty of Confidence: A duty of confidence arises when one person discloses information to another in circumstances where it is reasonable to expect that the information will be held in confidence.

Explicit Consent: A form of consent normally given orally or in writing and is where the patient makes a clear and positive indication that they understand the consequences of what they are agreeing to and are content with these consequences.

Legitimate relationship: A relationship that exists between a patient and an individual or group of record users involved in their treatment which provides the justification for those users to access a patient record.

Patient: People who are users of the Trust's services, also known as 'Service Users' or 'Clients'.

Personal Data: Data that relates to and identifies a living individual that can identify the individual from this data or other information in the possession of the data controller. This is also known as Person Identifiable Data (PID). **See Appendix A - Personal Data Flowchart**

Secondary Purpose: A purpose other than direct care such as healthcare planning, commissioning, public health, clinical audit and governance, benchmarking, performance improvement, medical research and policy development.

Special Category Data: Data that relates to a living individual that includes racial or ethnic origin, political opinions, religious or other philosophical beliefs, trade union membership, genetic data, biometric data, physical or mental health condition, sex life or sexual orientation, criminal proceedings or convictions**.**

Processing: Any operation or set of operations which are performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use,

disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Relevant Filing System: A structured set of information that can reference individuals either directly or indirectly.

Health Professional/Clinician: An individual registered by one of the professional organisations (GMC, NMC, HCPC) who provides health care services to a patient.

5. LEGISLATION

Portsmouth Hospitals NHS Trust has a legal obligation to comply with all appropriate legislation in respect of data, information, information security and confidentiality. The main pieces of legislation are listed below.

5.1 General Data Protection Regulations (GDPR) May 2018.

This EU legislation provides controls on the handling of personal identifiable information for all living individuals. In Article 5 of the GDPR the principles of processing are listed along with the principle of accountability and the duty of data controllers to demonstrate compliance to the following:

- Lawfulness, fairness and transparency
- Purpose limitation – data is collected for a specified, explicit and legitimate purpose and not further processed in a manner that is incompatible with those purposes
- Data minimisation – data should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- Accuracy – every reasonable step must be taken to ensure that personal data is correct and up to date. Inaccurate data may need to be erased or rectified without delay
- Storage limitation – data should be kept for no longer than necessary
- Integrity and confidentiality – protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

5.2 Data Protection Act (DPA) 2018

This UK Act supplements the GDPR and applies a broadly equivalent regime to certain types of processing to which the GDPR does not apply.

5.3 Access to Health Records Act 1990

This Act provides controls on the management and disclosure of health records for deceased persons. The personal representative of the deceased or a person who might have a claim arising from the patient's death can request access to the patient's data.

5.4 Common Law Duty of Confidentiality

Case law which prohibits the use and disclosure of information provided in confidence unless there is a statutory requirement or court order to do so. Such information may be disclosed only for purposes that the subject has been informed about and has consented to, provided also that there are no statutory restrictions on disclosure. This duty is not absolute, but should only be overridden if the holder of the information can justify disclosure as being in the public interest, for example to protect the vital interests of the data subject or another person or for the prevention or detection of a **serious** crime.

5.5 The Computer Misuse Act 1990

This Act makes it a criminal offence to access any part of a computer system, programs and/or data that a user is not entitled to access.

Employees are granted access to personal information on Trust systems for purposes related to their employment. Accessing your own or another person's information not related to your work is a breach of confidentiality and a breach of this policy. If you wish

to access your own or another persons medical information you must follow the Trust Access to Personal Records Policies.

The laws mentioned above are the main regulations which drive the data protection agenda. However there are many additional laws which may have an impact on data protection.

- Access to Medical Reports Act 1988
- Communications Act 2003
- Crime and Disorder Act 1998
- Data Retention (EC Directive) Regulations 2009
- Environmental Information Regulations (2004)
- Freedom of Information Act 2000
- Health and Social Care Act 2008
- Health and Social Care (National Data Guardian) Act 2018
- Human Rights Act 1998
- Mental Capacity Act 2005
- NHS Care Record Guarantee 2011
- Privacy and Electronic Communications Regulations 2003
- Public Records Act 1958
- Regulation of Investigative Powers Act 2000

6. NATIONAL GUIDANCE

6.1 Confidentiality: NHS Code of Practice 2003

This code provides detailed guidance for NHS bodies concerning confidentiality and patient's consent to use their health information. It also details the required practice the NHS must take concerning security, identifying the main legal responsibilities for an organization and also details employee's responsibilities.

6.2 Caldicott Reports

These reports provide guidance to the NHS on the use and protection of person identifiable data, and emphasizes the need for controls over the availability of such information and access to it. It makes a series of recommendations and identifies that all NHS organisations are to ensure that they have an appointed Caldicott Guardian who is responsible for compliance with the Caldicott Principles and Standards.

- Justify the purpose
- Don't use personal confidential data unless it is absolutely necessary
- Use the minimum necessary personal confidential data
- Access to personal confidential data should be on a strict need-to-know basis
- Everyone with access to personal confidential data should be aware of their responsibilities
- Understand and comply with the law
- The duty to share information can be as important as the duty to protect patient confidentiality

Additional guidance can be found in the following:

- CQC Safe data, safe care (2016)
- Data Retention (EC Directive) Regulations 2009
- Data Security Standards (2017)
- Data Security and Protection Requirements (2017)
- Information Security Management: NHS Code of Practice (2007)
- National Data Guardian for Health and Care Review of Data Security, Consent and Opt-outs (2016)
- NHS Constitution 2015
- Records Management Code of Practice for Health and Social Care 2016

- Review of Data Security, Consent and Opt-Outs NDG (2016)
- Safe data, safe care CQC (2016)
- The Employment Practices Code (ICO 2005)
- Your Data: Better security, better choice, better care DH (2017)

7. ROLES AND RESPONSIBILITIES

7.1 The Chief Executive (CE)

The Accountable Officer who is responsible for overall leadership and management of the Trust and has ultimate responsibility for ensuring compliance with the legislation. The Chief Executive is responsible for ensuring that the responsibility for data protection is allocated appropriately within the Trust and that the role is supported.

7.2 The Senior Information Risk Officer (SIRO)

The SIRO has overall responsibility for the organisation's Information Risk Policy and acts as the champion for information risk on the Board and provides written advice to the CE and the Board on its effectiveness. This is currently held by the Director for Governance and Risk.

7.3 The Caldicott Guardian

The Caldicott Guardian is an advisory role established to protect the confidentiality of patient information and ensure it is shared appropriately and securely. This currently sits with the Medical Director.

7.4 Head of Information Governance and Data Protection Officer

Informs and advises the Trust and its employees of their obligations under the GDPR; monitors compliance with the GDPR and Trust policies; provides advice on DPIA's; cooperates with the ICO; acts as the point of contact for the ICO on issues relating to processing and other matters. The Head of IG has a leadership role, maintaining the confidence of patients, staff and the public, through advice and guidance on the creation of robust and effective processes to protect and handle personal information.

7.5 IT Security Specialist

Provides advice on all aspects of electronic information security. Assesses the risks and threats and offers advice on controls to reduce the risks.

7.6 Information Governance Leads

Responsible for ensuring that IG is embedded at the local level, including reporting at DPDQ regarding their assets, information flows, contracts, sharing arrangements and compliance checklists

7.7 Divisional and Care Group Managers

Are responsible for the local implementation of this policy in their areas of responsibility.

7.8 All Staff

Everyone working for the NHS has a legal duty to keep information about patients and staff confidential. They are required to adhere to confidentiality agreements in their contract of employment, the NHS Confidentiality Code of Practice, the Common Law duty of Confidence and any professional codes of practice issued by their professional body.

8. GDPR PRINCIPLES

The Trust is a public authority which collects and processes vast quantities of personal and special category data. As such we are required to abide by all relevant legislation pertaining to Data Protection and Confidentiality. The main legislation governing Data Protection are the GDPR (2016) and the DPA (2018) both of which have recently been enacted.

The principles of the GDPR will be discussed individually along with the measures the Trust must take to ensure compliance with the law.

8.1 Lawfulness, fairness and transparency

- Ensuring that the legal basis for the processing of information is identified before processing commences.

- As a public authority which processes personal and special category information, the legal basis for processing information for the provision of direct care is identified as Article 6 (1)(c) and/or 9(2)(h) – **See Appendix B Legal Basis for Processing.**

- Ensuring the Trust's Privacy Notice (available on the Trust website) is kept up to date, and complies with the Information Commissioner's Office (ICO) Code of Practice. The Trust must have an appointed Data Protection Officer, whose contact details are available to the public.

- Complying with the common law duty of confidentiality; that any personal information given or received in confidence for one purpose may not be used for a different purpose or passed on to anyone else without the consent of the individual.

8.2 Purpose limitation – data is collected for a specified, explicit and legitimate purpose and not further processed in a manner that is incompatible with those purposes

- A Data Protection Impact Assessment (DPIA) is completed for the introduction of new processes or the updating of existing processes for collecting personal information. – **see Appendix C.**

- The DPIA must contain the purpose of the collection along with the legal basis for processing. Information collected for one purpose may not automatically be used for a second purpose.

- The DPIA must be ratified at the Data Protection and Data Quality (DPDQ) Committee before the new process or update can be applied.

8.3 Data minimisation – data should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

- Only data required for the specified legitimate purpose should be collected, nothing more.

- When completing a DPIA ask 'do I really need to collect this information; what does it add to my purpose?'

- Do not use person identifiable data when anonymous, pseudonymous or aggregate data will suffice.

8.4 Accuracy – every reasonable step must be taken to ensure that personal data is correct and up to date. Inaccurate data may need to be erased or rectified without delay

- The accuracy of the data recorded should be verified at every contact with the patient

- Data Quality Audits should be regularly undertaken to ensure that information recorded for the patient represents a true picture of their encounter with the Trust

- Inaccurate demographic data should be corrected immediately without delay. Inaccurate clinical data should not be erased if it forms part of the patient's hardcopy record. Follow guidance in the Health Records Management policy for appropriate correction techniques.

Inaccurate electronic data may be erased, as long as the system records this access and action.

- If a clinician has acted on the inaccurate data, then the inaccurate data should not be erased. A comment should be added to the patient record and the inaccuracy highlighted.

8.5 Storage limitation – data should be kept for no longer than necessary

- All staff responsible for the storage of patient personal information (electronic or hard copy) should follow the Records Management Code of Practice for Health and Social Care 2016 with regards to retention periods.

- All staff wishing to destroy personal data should contact the Health Records Manager, the IT Department or the Head of Information Governance to discuss the method of destruction.

8.6 Integrity and confidentiality – protection against unauthorised or unlawful processing and against accidental loss, destruction or damage

- All hardcopy personal information must be protected against inappropriate access. All staff must adhere to the 'Secure Handling of Personal Information policy'.

- Routine IG Compliance checks should be carried out by ward managers/matrons quarterly and results sent to the IG department.

- Random unannounced IG Compliance checks will be undertaken by the IG Team and/or Security.

- All electronic systems which store personal information should follow the Trust's IT Security Policy

8.7 Patient Rights under GDPR

The new legislation has expanded the rights of individuals with regard to their personal data. These rights are:

- **The right to be informed**. This encompasses the Trust's obligation to provide 'fair processing information' through the Privacy Notice. It emphasizes the need for transparency over how the Trust uses personal data.
- **The right of access.** This allows individuals to be aware of and verify the lawfulness of the processing. The Trust must supply a copy of the information free of charge.
- **The right to rectification.** This entails the correction of inaccurate or incomplete information. If this information has been disclosed to third parties, the third party must be informed of the rectification
- **The right to erasure (the right to be forgotten).** Enables the individual to request deletion or removal of personal data where there is no compelling reason for its continued processing. Information in a patient's health record is exempt from erasure
- **The right to restrict processing.** Individuals have a right to 'block' or suppress processing of personal data in some circumstances.
- **The right to data portability**. It allows individuals to move, copy or transfer personal data from one IT environment to another in a safe and secure way.
- **The right to object to processing** based on legitimate interests or the performance of a task in the public interest/exercise of official authority, direct marketing and for processes of scientific/historical research and statistics
- **Rights in relation to automated decision making and profiling**.

9. CONFIDENTIALITY

Health information which is collected from patients in confidence attracts the common law duty of confidentiality until it has been anonymized. This legal duty prohibits information use and disclosure without consent – effectively providing individuals with a degree of control over who sees information they provide in confidence. This duty can only be overridden if there is a statutory requirement, a court order, or if there is a robust public interest justification.

The 'Confidentiality: NHS Code of Practice' was published by the Department of Health and is a guide to required practice for those who work within or under contract to NHS organisations. The Code is relevant to anyone working in and around the health services.

The importance of maintaining confidentiality can be evidenced by its inclusion in all NHS staff employment contracts, in the NHS standard Terms & Conditions for procurement and in Codes of practice published by professional bodies such as the NMC, the GMC and the HSPC.

Portsmouth Hospitals NHS Trust is committed to ensuring that, as far as is reasonably practicable, the way we provide services to the public and the way we treat our staff reflects their individual needs and does not discriminate against individuals or groups on any grounds.

9.1 Exemptions to Confidentiality

In certain circumstances personal information may be disclosed and guidance is below. However it is vital in each case that staff make an assessment of the need to disclose the information and document that the information has been released to whom and for what reason. If they are in any doubt, they should seek advice from their Team Manager/Senior Clinician or the Caldicott Guardian.

9.2 Disclosing Information against the Subject's wishes

The responsibility to withhold or disclose information without the data subject's consent lies with the senior manager or senior clinician involved at the time and cannot be delegated.

Circumstances where the subject's right to confidentiality may be overridden are rare.

Examples of these situations are:

- Where the subject's life may be in danger, or cases in which s/he may not be capable of forming an appropriate decision
- Where there is serious danger to other people, where the rights of others may supersede those of the subject, for example a risk to children or the serious misuse of drugs
- Where there is a serious threat to the healthcare professional or other staff
- Where there is a serious threat to the community
- In other exceptional circumstances, based on professional consideration and consultation.

The following are examples where disclosure without consent is required:

- Births and deaths - National Health Service Act 1977
- Notifiable communicable diseases - Public Health (Control of Diseases) Act 1984
- Poisonings and serious accidents at the work place - Health & Safety at Work Act 1974
- Terminations - Abortion Regulations 1991
- Child abuse - Children's Act 1989 and The Protection of Children Act 1999
- Drug Addicts - Drugs (Notification of Supply to Addicts) Regulations 1973
- Road traffic accidents - Road Traffic Act 1988

- Prevention/detection of a serious crime e.g. terrorism, murder - The Crime and Disorder Act 1998

If in doubt, staff should seek guidance, in confidence, from a senior Clinician or Senior Manager, the Head of Information Governance, the SIRO or the Caldicott Guardian.

The Trust will support any member of staff, who after using careful consideration, professional judgement, and has sought guidance from their manager, can satisfactorily justify and has documented any decision to disclose or withhold information against a patient's wishes.

9.3 Non-Disclosure of personal information contained in a health record

An individual requesting access to their health records may be refused access to parts of the information if an appropriate clinician deems exposure to that information could cause physical or mental harm to the data subject or a third party.

Clinicians should be prepared to justify their reasons in a court of law if necessary. In all cases reasons for non-disclosure must be documented.

Where access would disclose information relating to or provided by a third party, consent for release must be sought from the third party concerned, unless that third party is a health professional who had provided the information as part of their duty of care or in the course of their employment. Where the third party does not consent, the information may be disclosed provided the identity of the third party is not revealed.

The Information Commissioner's Code of Practice suggests that this might be done by omitting names and identifying particulars from the records. Care should be taken to ensure that the information if released is genuinely anonymous. Further guidance is available in the Access to Personal Records Policy (Patient/Employee).

9.4 Personal Identifiable Data in Medical Research

All project based research within the Trust must comply with the Data Protection & Caldicott Guardian Principles as set out within this Policy, be registered by the Research and Development Department and undergo review through the NHS Health Research Authority (HRA) approval process to provide assurance to our Trust, our patients and the public that all research meets the necessary legal and compliance standards.

The legal basis for processing confidential data for health and social research is '**a task in the public interest'**; (6(1)(e) – processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller'

The Research & Development Department will log and retain as appropriate, all relevant data protection agreements and HRA approvals for research studies, as evidence for compliance with the General Data Protection Regulation 2018.

10. The National Opt Out

In 2016 The National Data Guardian proposed that 'there should be a new consent/opt-out model to allow people to opt-out of their personal confidential data being used for purposes beyond their direct care.'

All reporting data sets which identify individuals will need to ensure that anyone who has opted out nationally is not included in the data set when it is sent out. This includes many of the national registries, national audits, research and service planning data. This applies to any data collected without consent under a section 251 issued by the Confidential Advisory Group.

To understand how to comply with the National Opt Out contact the Information Governance Team.

10. DATA PROTECTION IMPACT ASSESSMENTS AND DUE DILIGENCE

All projects and processes that involve processing personal information or intrusive technologies give rise to privacy issues and concerns. To enable the Trust to address the privacy concerns and risks, the GDPR requires a Data Protection Impact Assessment (DPIA) be completed, and signed off by the Data Protection Officer and/or the DPDQ Committee. Refer to Privacy Impact Assessment Procedure and Template for details.

11. FINANCIAL IMPACT AND RESOURCE IMPLICATIONS

The Trust is required to be compliant with the NHS Digital Data Security and Protection Toolkit. Failure to maintain this would mean that the Trust would be unable to tender for new business.

Additionally, the Information Commissioners Office monitors all serious breaches of personal information and/or confidentiality, and could impose a fine of up €20,000,000 (approx. £17m) or 4% of the Trust's annual turnover.

12. MONITORING COMPLIANCE

Data Security and Protection Toolkit:
The Trust is required to complete an annual review of Information Governance compliance by completing the on-line NHS Digital Data Security and Protection Toolkit.

Reporting IG Breaches
One of the requirements of the GDPR is that the Trust must use appropriate technical and organizational measures, to ensure that personal data is processed in a manner to ensure the appropriate security of the data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage.
Breaches can be categorized as:

- Confidentiality breach – unauthorized or accidental disclosure of, or access to personal data
- Availability breach – where there is an accidental or unauthorized loos of access to or destruction of, personal data.
- Integrity breach – where there is an unauthorized or accidental alteration of personal data.

Data breaches can have a range of significant adverse effects on individuals which can result in physical, material or non-material damage.

The GDPR 2016 and DPA 2018 introduce a duty on all organizations to report certain types of personal data breach to the ICO and or the Department of Health and Social Care. A breach must be notified within 72 hours. If the breach is likely to result in a high risk to the rights and freedoms of individuals, the Trust must also inform those individuals without undue delay.

Grading the personal data breach
Any incident must be graded according to the significance of the breach and the likelihood of those serious consequences occurring. The incident must be graded according to the impact on the individual or groups of individuals and not the organisation. It is advisable that incidents are reviewed by the Data Protection Officer or Caldicott Guardian or the

Senior Information Risk Owner when determining what the significance and likelihood a data breach will be.

The significance is further graded rating the incident of a scale of 1-5. 1 being the lowest and 5 the highest.

The likelihood of the consequences occurring are graded on a scale of 1-5 1 being a non-occurrence and 5 indicating that it has occurred.

Establish the likelihood that adverse effect has occurred:

No.	Likelihood	Description
1	Not occurred	There is absolute certainty that there can be no adverse effect. This may involve a reputable audit trail or forensic evidence
2	Not likely or any incident involving vulnerable groups even if no adverse effect occurred	In cases where there is no evidence that can prove that no adverse effect has occurred this must be selected.
3	Likely	It is likely that there will be an occurrence of an adverse effect arising from the breach.
4	Highly likely	There is almost certainty that at some point in the future an adverse effect will happen.
5	Occurred	There is a reported occurrence of an adverse effect arising from the breach.

If the likelihood that an adverse effect has occurred is low and the incident is not reportable to the ICO, no further details will be required.

Grade the potential severity of the adverse effect on individuals:

No.	Effect	Description
1	No adverse effect	There is absolute certainty that no adverse effect can arise from the breach
2	Potentially some minor adverse effect or any incident involving vulnerable groups even if no adverse effect occurred	A minor adverse effect must be selected where there is no absolute certainty. A minor adverse effect may be the cancellation of a procedure but does not involve any additional suffering. It may also include possible inconvenience to those who need the data to do their job.

3	Potentially some adverse effect	An adverse effect may be release of confidential information into the public domain leading to embarrassment or it prevents someone from doing their job such as a cancelled procedure that has the potential of prolonging suffering but does not lead to a decline in health.

4	Potentially Pain and suffering/ financial loss	There has been reported suffering and decline in health arising from the breach or there has been some financial detriment occurred. Loss of bank details leading to loss of funds. There is a loss of employment.
5	Death/ catastrophic event.	A person dies or suffers a catastrophic occurrence

The breach assessment grid operates on a 5 x 5 basis with anything other than “grey breaches” being reportable. Incidents where the grading results are in the red are advised to notify within 24 hours.

Severity (Impact)	Catastrophic	5	5	10	15	20	25
	Serious	4	4	8	12	16	20
	Adverse	3	3	6	9	12	15
	Minor	2	2	4	6	8	10
	No adverse effect	1	1	2	3	4	5
			1	2	3	4	5
			Not Occurred	Not Likely	Likely	Highly Likely	Occurred
			Likelihood that citizens' rights have been affected (harm)				

All incidents which involve a breach of confidentiality, availability and/or integrity which are scored 6 or higher must have an action plan recorded on the Trust's incident reporting system. For further information see NHS Digital 'Guide to the Notification of Data Security and Protection Incidents'.

Care Quality Commission (CQC) Well Led Inspections
Since September 2017 the CQC's well led inspection framework will include the importance of meeting the data security standards set out by the National Data Guardian. For more information see 'CQC Safe data, safe care July 2016'.

13. TRAINING REQUIREMENTS

The Head of Information Governance has overall responsibility for maintaining training and awareness of confidentiality and information security issues for all staff. However, the Trust Caldicott Guardian is also able to provide advice on the sharing of, and access to, patient identifiable information.

Information Governance training is mandatory and all new starters must receive IG training as part of their corporate induction.

All staff members are required to undertake specialist Information Governance training as appropriate to their role.

Information Governance training must be completed on an annual basis by all staff. See **Appendix D Trusts Training Needs Analysis**

14. REFERENCES AND ASSOCIATED DOCUMENTATION

- General Data Protection Regulations (2016) European Union
- The Data Protection Act (2018)
- The Access to Health Records Act (1990)
- 2017/18 Data Security and Protection Requirements (2017) Department of Health/NHS England
- Safe Data, safe care (2016) CQC
- Review of Data Security, Consent and Opt-Outs (2016) National Data Guardian for Health and Care
- Guide to Notification of Data Security and Protection Incidents (2018) NHS Digital
- Confidentiality: NHS Code of Practice (2003/2010) Department of Health
- The Care Record Guarantee (2011) NHS England
- Records Management Code of Practice for Health and Social Care (2016) Information Governance Alliance

15. EQUALITY IMPACT STATEMENT

Portsmouth Hospitals NHS Trust is committed to ensuring that, as far as is reasonably practicable, the way we provide services to the public and the way we treat our staff reflects their individual needs and does not discriminate against individuals or groups on any grounds.

This policy has been assessed accordingly

Our values are the core of what Portsmouth Hospitals NHS Trust is and what we cherish. They are beliefs that manifest in the behaviours our employees display in the workplace.

Our Values were developed after listening to our staff. They bring the Trust closer to its vision to be the best hospital, providing the best care by the best people and ensure that our patients are at the centre of all we do.

We are committed to promoting a culture founded on these values which form the 'heart' of our Trust:

Working together for patients
Working together with compassion
Working together as one team
Working together always improving

This policy should be read and implemented with the Trust Values in mind at all times.

16. MONITORING COMPLIANCE WITH PROCEDURAL DOCUMENTS

This document will be monitored to ensure it is effective and to assure compliance.

Minimum requirement to be monitored	Lead	Tool	Frequency of Report of Compliance	Reporting arrangements	Lead(s) for acting on Recommendations
DSP Toolkit	Head of IG	NHS Digital DSPT website	Yearly	Policy audit report to: • DPDQ & Board	Head of IG SIRO
Data Quality Audit	Head of IS	Local collection tool	Yearly	Policy audit report to: • DPDQ	Head of IS
IG Breaches	Head of IG	Datix	Monthly	Policy audit report to: • DPDQ	Head of IG SIRO Caldicott Guardian Risk
SAR responses	Head of IG	Local collection tool	Monthly	Policy audit report to: DPDQ	Head of IG Health Records Manager HR Legal

EQUALITY IMPACT SCREENING TOOL

To be completed and attached to any procedural document when submitted to the appropriate committee for consideration and approval for service and policy changes/amendments.

Stage 1 - Screening			
Title of Procedural Document: Caldicott, Confidentiality and Data Protection Policy			
Date of Assessment	28/02/2019	**Responsible Department**	Information Governance
Name of person completing assessment	E Armour	**Job Title**	Head of Information Governance and Data Protection Officer

Does the policy/function affect one group less or more favourably than another on the basis of :	**Yes/No**	**Comments**
• Age	No	
• Disability	No	
• Gender reassignment	No	
• Pregnancy and Maternity	No	
• Race	No	
• Sex	No	
• Religion or Belief	No	
• Sexual Orientation	No	
• Marriage and Civil Partnership	No	
If the answer to all of the above questions is NO, the EIA is complete. If YES, a full impact assessment is required: go on to stage 2, page 2		
More Information can be found be following the link below www.legislation.gov.uk/ukpga/2010/15/contents		

Stage 2 – Full Impact Assessment			
What is the impact	**Level of Impact**	**Mitigating Actions** (what needs to be done to minimise / remove the impact)	**Responsible Officer**

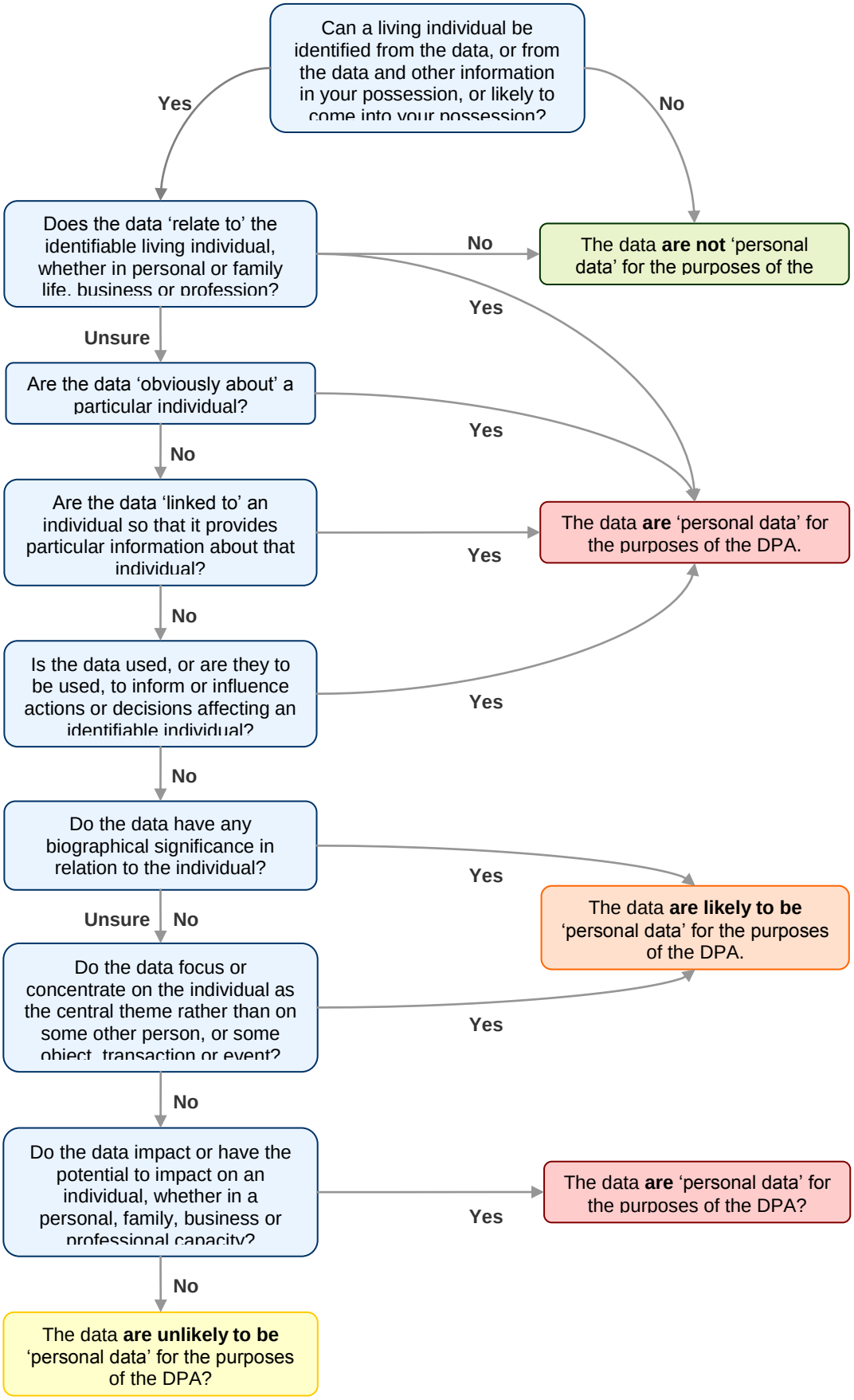
Monitoring of Actions

The monitoring of actions to mitigate any impact will be undertaken at the appropriate level

Specialty Procedural Document:	Specialty Governance Committee
Clinical Service Centre Procedural Document:	Clinical Service Centre Governance Committee
Corporate Procedural Document:	Relevant Corporate Committee

All actions will be further monitored as part of reporting schedule to the Equality and Diversity Committee

Appendix 1: Personal Data Flow Chart



Appendix 2: Legal Basis for Processing

Processing Personal Data Article 6(1) GDPR

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

Processing Special Category Data Article 9(2) GDPR

(a) the data subject has given **explicit consent** to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

(e) processing relates to personal data which are manifestly made public by the data subject;

(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Appendix 3: Data Protection Impact Assessment (DPIA)

QAH
QUEEN ALEXANDRA Hospital

Portsmouth Hospitals NHS
NHS Trust

Data Protection Impact Assessment (DPIA) Screening Questionnaire

Projects or activities that involve processing or sharing personal data/information or commercially sensitive data/information give rise to privacy issues and concerns. To enable the Trust to address these privacy concerns, a Data Protection Impact Assessment (DPIA) can be used to assess privacy risks to individuals in the collection, use, storage, disclosure and disposal of data/information. The DPIA can help identify privacy risks, foresee problems and bring forward solutions.

Title of Project:	

Brief Description of Project:	

Does my project need a DPIA? Does it include:

- A new service/system/procedure
- A change to an existing service/system/procedure
- New projects or activities
- Changes to existing projects/procedures/systems
- A data sharing initiative where two or more organisations seek to pool or link sets of personal data
- A proposal to identify people in a particular group or demographic and initiate a course of action
- Using existing data for a new and unexpected or more intrusive purpose.
- Information Sharing Protocols
- Relocation of staff or equipment
- Stakeholder engagement e.g. surveys

If this is a change to an existing service/system/procedure please provide the original PIA if available.

Contact Details:

Name	
Designation	
CSC/Dept.	
Telephone	
Email	

Please answer the following questions in relation to the proposal:		Yes	No
Q1	Will the project involve the collection of new information about individuals?		
Q2	Will the project compel individuals to provide information about themselves?		
Q3	Will information about individuals be disclosed to organisations or people who have not previously had routine access to that information?		
Q4	Will information about individuals be used for a purpose it is not currently used for or in a way it is not currently used?		
Q5	Will information be entered into an electronic system (web based or otherwise)?		
Q6	Will the project introduce new technology which might be perceived as intrusive? E.g. use of CCTV, sound and vision recording, processing of biometric information.		
Q7	Will the project result in decisions being made about individuals which might have a significant impact on them?		
Q8	Does the project involve the processing of particularly sensitive information? e.g. detailed clinical records, child protection records, fertility or genetic information.		

If the answer to one or more of the above questions is **YES,** a detailed DPIA will need to be undertaken.
If the answers to **all** of the above questions are **NO,** you do not need to complete a full DPIA.
Please send this page to information.governance@porthosp.nhs.uk as a record of the assessment.
If you require assistance filling in this form, please contact the Trust's IG Manager on ext. 3708

QAH
QUEEN ALEXANDRA Hospital

Portsmouth Hospitals NHS
NHS Trust

Data Protection Impact Assessment

Date of Submission: _____

1.0 Project Details	
Project Name	
Name and Job title of person submitting this DPIA	
Contact details of person submitting this DPIA telephone/email	
CSC/Department involved in the Project	
Executive Sponsor	
Brief description of project.	
Why is this DPIA needed?	
Why is the new system/change required?	
Does the project involve multiple organisations? Please provide the name of the project lead and contact details.	
Key Stakeholders	
Overall Benefits:	

Overall Constraints:	
IT Lead on Project	
If new or changing technology is involved has an IG/ Security - Due Diligence Risk Assessment been completed by IT?	**Note:** In situations where new and changing technology is involved due diligence must be completed before the DPIA can be considered. **Do Not** submit the DPIA until the due diligence has been completed by IT.
Finance Lead	
Has a Business Case been signed off by the Business Case Review Group?	
Procurement Lead	
Is there a contract in place? If yes provide reference number	
System Users	
Who is the Information Asset Owner?	
Who is the Information Asset Administrator?	
Is a System Level Security Policy in place or required?	
Who is responsible for the information? Who will be the Data Controller?	
What is the process for start-up and closing down this piece of work?	

2.0 Information Collection & Use

Will this project involve the collection of data?	**YES** ☐ **NO** ☐ IF **NO** go to 4.0 Sharing of Information	
Please describe what type of information will be collected?	Personal (PID, PCD)	
	Sensitive Personal	
	Corporate Confidential	
	Pseudonymised	
How will this information be collected?	Paper	
	Electronic	

	Electronic (automated)	
	Other	
How will this information be used?		
If information is being collected or purpose for collection is changing, how is it changing and what will be different?		
What Legal Basis are you proposing to use for the collection / processing of this information?		
Are you proposing to link data sets in order to achieve project aims? If yes, please detail linkages.		
What reports will be generated from this information? Will the reports be anonymous, pseudonymous or identifiable? Please provide details?		
How is the information to be edited or deleted?		
How is the data quality to be checked?		
3.0 Storage/Retention/Disposal		
Where will the information be stored? Provide details of backups or copies that will be maintained.		
How will the information be stored?		
How long is the information to be retained for?		
What are the arrangements for disposal when the minimum retention period has been reached? Archived / Deletion / Destruction		
If the organisation/service ceases to operate, what will happen to the information?		

4.0 Sharing of Information	
Will the project involve the sharing of information?	**YES** **NO**
What information is being shared?	
Why is this information being shared?	
Who is the information to be shared with?	
What is the legal basis for the processing/sharing of the information?	
How will information be transferred or transported? SFTP, secure email, by hand etc.	
What are the Data Flows? (Please detail and attach a data flow diagram)	
What information sharing protocols and operational agreements are or will be in place to support this sharing?	
Does this activity propose to use information that may be subject to or require approval from NHS Digital?	
If using NHS Digital information is the new use covered by the purposes agreed under the existing ISA?	
5.0 Access to Information	
Which staff (roles) will have access? Will restrictions be based on different roles?	
How will information be accessed?	
How will access be controlled / monitored? e.g. audits/logs	
Will the system (electronic) be capable of recording details of access to the record and when?	
What training for staff is	

required for this project?	
Are you proposing to use a third party/data processor/system supplier as part of this project?	
Is the third party / data processor registered with the ICO? If not what IG assurances can the third party provide?	
Does the contract with the third party supplier contain all the necessary IG clauses?	
Is there or will there be an Information Sharing Agreement (ISA) in place with the third party supplier?	
Has the third party supplier been identified in any relevant ISA with NHS Digital?	
Who will be responsible for monitoring the contract / ISA with the third party supplier?	
Is the use of Cloud technology being considered either by you or a 3rd party supplier?	
Are you transferring any personal/sensitive information outside the EEA?	
Can the information be viewed / accessed online by people based outside the UK? If yes please provide details?	
6.0 Data Subject Awareness & Consent	
Is Consent from the data subject required?	
What is the process for obtaining and recording consent/dissent from the data subject?	
If consent has not been obtained or is not required is there a legal basis to share the information?	
What changes have been made or are proposed to	

Fair Processing Notices of the organisations involved?	
How can the Data Subject access any information relating to them as a result of this project?	

7.0 Business Continuity Plan

What business continuity plans are in place to protect the information?	

8.0 Additional Information / Comments

9.0 IG Leads Comments

I G Manager	
IT Department Lead	
Business Intelligence Lead	

Procurement Lead	

.

Outcome of IG Panel

Based on the information contained in this DPIA along with any supporting documents, the outcome is as follows:

Reviewed with no further recommendations:

Reviewed with recommendations / actions (list the recommendations / actions):

Reviewed and recommended not to proceed at present: (provide brief summary of reason)

Signed and approved on behalf of the Data Protection Officer:

Name: …….

Job Title: …….

Signature: …….. Date: …….

Signed and approved on behalf of Senior Information Risk Owner
Name: …….

Job Title: …….

Signature: …….. Date: …….

Signed and approved on behalf of the Caldicott Guardian

Name: …….

Job Title: …….

Signature: …….. Date: …….

Please note:

Where further evidence has been requested by PHT's DPIA panel, in cases where the original recommendation has been assessed as either *'Reviewed with recommendations' (and a further review is needed)* or '*Reviewed and recommended not to proceed at present'* this must be received by the DPIA Panel within a maximum timeframe of three months from the date of original submission. If the required evidence is not received in this timeframe the DPIA will be closed.

It is the responsibility of the Project/Activity Lead to notify the appropriate Information Asset Owner / Information Asset Administrator for inclusion on the Information Asset Register and Data Flow Mapping.

Date entered onto IG Asset Register & Data Flow Map: …….

Appendix 4: Trust Training Needs Analysis for Information Governance

Course	*Target Staff Group*	*Access*	*Frequency*
PHT Corporate Induction **(required)**	All PHT new starters All Engie new starters All MOD new starters	Paper – Induction Handbook Internet/intranet via Moodle	Once
Cyber Security Awareness – Level 1 on ESR **(required)**	All PHT staff All Engie staff All MOD staff Non-Executive Directors Bank, agency staff, Volunteers	Internet/intranet via ESR E-Learning	Yearly
Introduction to Risk Management for SIROs and IAOs (Workbook & PowerPoint) **(required)**	SIRO IAO	PowerPoint and workbook based specialist training for individual staff	SIRO – yearly IAO's – once
The Role of the Caldicott Guardian **(required)**	Caldicott Guardian	PowerPoint and workbook based specialist training for individual staff or externally provided course	Once
Access to Health Records (Workbook & PowerPoint)	All HRL staff who handle SAR's	PowerPoint and workbook based specialist training for individual staff	Once
Clinical Coding Standards Training Course	All clinical coding staff	Classroom	Within 6 months of recruitment
Clinical Coding Refresher Training	All clinical coding staff	Classroom	Every 3 years
Clinical Coding Trainer Refresher course	Head of Clinical Coding	Classroom	Every 3 years
TAP Re-assessment	Head of Clinical Coding	Observation Assessment	Every 3 years

National Registration Authority and Smartcard Policy **(required)**	All staff involved with issuing RA smartcards	NHS Digital Card Identity System	Once
Medico Legal & Registration Training Manual	All HRL staff who handle SAR's	Paper Electronic	Yearly by HRL staff
PHT CfH stand alone IG Annual Training modules (Beginner, Introduction, Refresher)	All staff	Internet/intranet via ESR	Ad hoc
Information Governance Awareness Induction training (required)	All Student Nurses/AHP/HCS on University Placements	20 min presentation & group discussion by L & D	On commencement of placement
UK Core Skill Training Framework (required)	All Student Nurses/AHP/HCS on University Placements prior to placement	Internet	On commencement of training
LINK entry	All staff	Electronic or paper	As required
Staff Briefs (ad hoc email notices/pop ups)	All staff	Electronic	As required
Quick reference guides, staff guidance documents and staff information leaflets	All staff	Electronic, IG Intranet page	As required
Staff Handbook	All staff	Paper	Yearly
Training by request (tailor made awareness sessions)	Ad hoc staff teams and management groups	Face to face - group sessions by arrangement with IG lead	On request
Spot check/ audits/Advice & guidance	Individual staff Teams	Spot check schedule By request	Random