Data Protection Impact Assessment

Title	Ref number
Prognostic and molecular classification of breast cancer for personalised therapy	

Introduction

A Data Protection Impact Assessment enables Sherwood Forest Hospitals NHS Foundation Trust (SFHFT) to meet its legal/compliance obligations with the Data Protection Act 2018 and the General Data Protection Regulation 2016.

The Data Protection Impact Assessment (DPIA) ensures the confidentiality, integrity and availability of information by applying a risk management process and gives confidence to interested parties that risks are adequately managed, as required under ISO/IEC: 27001:2017. It is important that the DPIA is part of and integrated with the organisation's processes and overall management structure and that information security is considered in the design of processes, information systems, and controls. The process identifies and allows issues to be mitigated at an early stage of implementation/change thereby reducing associated costs and damage to reputation. Data Protection Impact Assessment are an integral part of the "privacy by design" approach as identified by the Information Commissioner's Office.

Document Completion

A DPIA must be completed wherever there is **a change to an existing process or service** or **if a new process or information asset is introduced** that is likely to involve a new use or significantly changes the way in which personal data, special categories of personal data or business critical information is processed.

This document, and the privacy risks, actions and recommendations identified within it, will be accepted in the Project Sign Off (page 3). The project will need to signed off by the Information Asset Owner, a representative from NHIS, Information Governance/Data Protection Officer and a customer representative (if applicable) and through the appropriate governance structure of the implementing organisation. Sign off and acceptance of the document does not close the privacy risks related to this project. It is important that the risks are revisited during the life of the project and any additional privacy risks identified are appropriately reviewed and mitigated.

PLEASE NOTE:
The Information Asset Owner (implementer) undertaking the Data Protection Impact Assessment has a responsibility to ensure that Patient Safety, Technical Security and Quality Impact Assessments are considered, in line with the Trust procedures.
Assessment Process Stages

Activity	IAO	Governance
Complete Title Bar and include Ref Number	✓	

Complete Project Details and check the Initial Screening Questions	✓	
Complete Stage 1 – Introductory meeting and review Initial Screening Questions and follow up questions to determine if a Stage 2 – DPIA (Full) is to be undertaken	✓	
Initial Screening Questions to be formally written up and Introductory Meeting to be formally recorded		

If a Data Protection Impact Assessment **IS NOT** required		
Activity	**IAO**	**Governance**
Complete Assessment Summary & Recommendations for Action		
Assessment to be passed to Implementer		
Ensure Sign Off is completed		
Assessment shared with customer if appropriate		
Assessment to be kept with project documentation copy to Information Governance		

OR

If a Data Protection Impact Assessment **IS** required		
Activity	**Implementer**	**Governance**
Complete Stage 2 – Data Protection Impact Assessment (Full)	✓	✓
Complete Stage - 3 Work Flow Mapping	✓	
Complete Stage - 4 Identified Risks and Mitigating Action	✓	✓
Complete Stage – 5 Legal Compliance		✓
Complete Assessment Summary & Recommendations for Action		✓
Closure meeting for final agreement	✓	✓
Ensure Sign Off is completed		✓
Assessment shared with customer if appropriate		✓
Assessment to be kept with project documentation copy to Information Governance		✓

This document is intended to be completed by the Trust and external organisations the *Governance* section will be completed by the IG Team with support from the relevant NHIS specialist teams as applicable.

Project Details

Project Title:	Prognostic and molecular classification of breast cancer for personalised therapy

Project Description: Describe in sufficient detail for the proposal to be understood

The Breast Pathology Research Group at the University of Nottingham has a long standing national and international track record in breast cancer diagnosis, prognostic and predictive stratification. From its beginning in the 1970s we have generated research using over 600 biomarkers, achieved more than 700 publications in peer- reviewed journals, and several books and book chapters have been based on our research output.

The aim of this proposal is to extend our research activity into determining the key mechanisms/roles and drivers controlling breast cancer behaviour and prognosis in an attempt to refine classification of breast diseases and to address gaps in current management strategies.

We have access to a local breast cancer cohort as part of the ethically approved research projects (REC reference 19/EM/0162 and REC reference 19/YH/0293) which comprise a cohort of patients who presented to Nottingham University Hospitals NHS Trust with breast lesions and received surgical treatment.

In this application we aim to extend our research on breast cancer and its precursor lesions using an additional cohort which comprises around 6,000 cases from Sherwood Forest Hospitals NHS Foundation Trust and to establish long term collaboration between the University of Nottingham and Sherwood Forest Hospitals NHS Foundation Trust.

The rationale of using this additional cohort of cases is to allow subgroup analysis and facilitate training and validation of digital pathology and other postgraduate student-related research. This will provide more reliable results for the clinical and research communities.

Inclusion criteria for this study:

- Patients presenting with breast cancer and its precursor lesions at the Sherwood Forest Hospitals NHS Foundation Trust. between 1st January 2000 - 31st December 2015.
- Age range: Lower limit 18 years – upper 100 years
- Availability of tissue material surplus to diagnostic pathology needs.
- Availability of linked metadata.

In our endeavour to identify novel diagnostic, prognostic and predictive biomarkers in breast cancer, we will:

1. Refine the criteria of breast cancer diagnosis and grading in the era of digital pathology

2. Use computational pathology and the power of machine learning and artificial intelligence, with the help of internal and external computer scientists' collaborators, to evaluate various morphological features in breast cancer whole slide images (WSIs) that cannot be assessed by visual inspection to provide objective algorithms for breast cancer diagnosis and prognosis.

3. Interrogate publicly available molecular datasets to utilise the power of gene expression microarrays and next generation sequencing which provide data on tens of thousands of genes. We will use various statistical and bioinformatics approaches to decipher these databases and to identify novel targets for further investigation and validation using the tissue microarray technology and different analytical techniques.

Overview of the proposal: What the project aims to achieve
The principal research question of this study is whether identification of distinctive morphological and genetics characteristics of breast cancer and its precursor's lesions can improve our understanding of the breast cancer biology. Our primary objective is to better classify breast cancer and its precursor lesions and to provide robust methods to predict its behaviour, outcomes and response to therapy, using this to improve personalised management of patients with breast disease.

Implementing Organisation:	Sherwood Forest Hospitals NHS Foundation Trust

Staff involved in DPIA assessment (Include Email Address):	Dr Muhammed Gill Consultant Histopathologist & Head of Service Muhammad.gill@nhs.net Alison Steel Head of Research and Innovation alison.steel1@nhs.net Clair Sleney Histopathology Lab Manager clair.sleney@nhs.net Fiona Haynes NIHR Research Advocate – PPI

	fiona.haynes123@btinternet.com Prof Emad Rakha Professor of Breast Pathology, University of Nottingham and Consultant Pathologist, Nottingham University Hospitals Trust emad.rakha@nottingham.ac.uk Dr Michael Toss Research Fellow, Breast Pathology Research Group (BPRG), University of Nottingham Michael.toss@nottingham.ac.uk Jenny Baldwin Research Projects Officer, Breast Pathology Research Group (BPRG), University of Nottingham Jennifer.baldwin@nottingham.ac.uk

Project Sign Off

	Name	Job Title	Organisation	Date
Information Asset Owner	Elaine Torr	Divisional General Manager	Sherwood Forest Hospitals NHS Foundation Trust	23rd April 2021
Data Protection Officer	Jacquie Widdowson	Information Governance Manager	Sherwood Forest Hospitals NHS Foundation Trust	23rd April 2021
Information Governance	Gina Robinson	Information Security Officer	Sherwood Forest Hospitals NHS Foundation Trust	14th April 2021
Senior Information Risk Owner	Paul Robinson	Chief Financial Officer	Sherwood Forest Hospitals NHS Foundation Trust	23rd April 2021

Caldicott Guardian	Shirley Higginbotham	Director of Corporate Affairs	Sherwood Forest Hospitals NHS Foundation Trust	**26th April 2021**
Chief Clinical Information Officer	David Selwyn	Medical Director	Sherwood Forest Hospitals NHS Foundation Trust	**27th April 2021**

Assessment Summary

To be completed by Information Governance

Outcome of Data Protection Impact Assessment:	
1. Project/Implementation is recommended **NOT** to proceed, as significant corporate/customer risks have been identified.	☐
2. Project/Implementation to proceed once identified risks have been mitigated as agreed.	☒
3. Project/Implementation has met required legislative compliance and poses not significant risks. No further action required.	☐

Summary of Data Protection Impact Assessment; including legislative compliance and identified risks:
Summary: The University of Nottingham is applying for section 251 authorisation (April 2021) to undertake this retrospective research study on 6000 Trust patients. If the application is rejected the research study would not have a legal basis in order to proceed. **Summary of Risks**: 1. Unintended release of data set beyond project recipient. 2. Failure of the de-identification of data process 3. University of Nottingham misuses the Trust's personal data, eg. by trying to re-identify individual's 4. Infringement of data subject rights and freedoms 5. The University of Nottingham is applying for section 251 authorisation (April 2021) to undertake this retrospective research study on 6000 Trust patients. If the application is rejected the research study would not have a legal basis in order to proceed.

Recommendations for Action

Summary of Identified Recommendations:		
Recommendations:	**Recommendation Owner:**	**Agreed Deadline for action:**
1. **Unintended release of data set beyond project recipient**. Data sets are subject to comprehensive arrangements for secure storage and transfer. Contracts and data sharing agreements to be in place forbidding the sharing of these data beyond the intended recipient. Data recipient due diligence identifies no concerns. Contracts in place to ensure on-going compliance for data use and sharing. Data set has been pseudonymised to a very high level to minimise the impact to data subjects should an inadvertent disclosure or loss of data occur.	IAO	To be agreed once the outcome of the Confidentiality Advisory Group application is known

Recommendations:	Recommendation Owner:	Agreed Deadline for action:
2. **Failure of the de-identification of data process** Pseudonymised data sets will be checked by two people before release to researchers.	IAA, Clair Sleney	No suitable date, this risk will be monitored throughout the lifecycle of the project
3. **University of Nottingham misuses the Trust's personal data, eg. by trying to re-identify individual's** At data collection stage the data subjects are identifiable through the linking mechanism; the linking table is held securely and separately within the confines of a separate folder controlled by the Trust's IT system and away from the data itself. Once pseudonymised, all data is held and transferred securely. Researchers are prohibited from attempting any re-identification and bound by contract to inform the Trust should the data be found to be identifiable.	IAA, Clair Sleney	No suitable date, this risk will be monitored throughout the lifecycle of the project

4. **Infringement of data subject rights and freedoms**. Confidentiality Advisory Group (CAG) approval is currently being applied for. Strong technical controls are in place to protect these data and the applied de-identification limits risk to data subject privacy.	IAA, Clair Sleney	No suitable date, this risk will be monitored throughout the lifecycle of the project
5. **The University of Nottingham is applying for section 251 authorisation (April 2021) to undertake this retrospective research study on 6000 Trust patients. If the application is rejected the research study would not have a legal basis in order to proceed.** Confidentiality Advisory Group (CAG) approval is currently being applied for.	IAO	No suitable date as this is driven by external parties. This risk will be monitored throughout the lifecycle of the project

Stage 1 – Initial Screening Questions

Answering "**Yes**" to a screening questions below represents a potential IG risk factor that may have to be further analysed to ensure those risks are identified, assessed and fully mitigated. The decision to undertake a full DPIA will be undertaken on a case-by-case basis by IG.

Q	Screening question	Y/N	Justification for response
1	Will the project involve the collection of information about individuals?	Y	Case information relating to the tumour - demographics, clinical and pathology data  DPIA%20Appendix%201%20-%20Fields%20
2	Will the project compel individuals to provide information about themselves?	N	
3	Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	Y	Data and tissue relating to the tumour from the retrospective cohort will be released to researchers and others with a particular expertise or facilities for analysis in a pseudonymised form. No contact with any of the patients included in this project is intended throughout the study period.
4	Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	Y	The information is being used for research and patients were not asked for consent for this at the time of their surgery.
5	Are there processes in place to ensure data is relevant, accurate and up-to-date?	Y	Data that is being analysed is historical. Only the Data Management Team have access to this and can identify which cases are relevant for the study. The team is trained on which systems to use to identify relevant data for the study. Researchers will have no access to the coding system linking patient data with transformed research data.
6	Are there security arrangements in place while the information is held?	Y	Data on the Trust's system is encrypted. All records are accessed by a Data Team, who are not researchers and who hold an NHS Honorary Contract. Data is held on the Trust's system where it is

Q	Screening question	Y/N	Justification for response
			pseudonymised. At this point it transfers to the University of Nottingham and is held on their secure servers with limited access to the authorised researchers and students. Only the Data Management Team (University specified individuals with letter of authority (LOA) and Trust specified individuals) have access to the pseudonymisation key to link data to a record. Identifiable patient data will not be moved outside of the confines of the Trust's IT system. Please note: The Data Management Committee comprise the medical laboratory assistant who will be employed by the Trust (funded by University of Nottingham) and 2 named individuals from University of Nottingham who hold letter of authority (LOA) research passport contracts.
7	Does the project involve using new technology to the organisation?	N	The data will be interrogated by the Data Management Team using existing systems and software.
8	Will the project result in you making decisions or taking action against individuals in ways which could have a significant impact on them?	N	The research output will help better understanding for breast cancer biology and behaviour; however there is no direct impact or any contact with patients whose samples included in this proposal. Nothing will affect their current management or clinical care.
If you have answered "Yes" to any of the questions numbered 1-8 please proceed and complete stage 2.			
9	Is a Patient Safety Review required?	N	Not required. This project is not patient facing.
10	Is a Quality Impact/Technical Security Review required?	Y	

Please ensure that on completion this is returned to Information Governance lead to agree how to proceed.

Stage 2 – Data Protection Impact Assessment

2.1	What is the change					
	New purpose?	☒	Revised/changed?	☐	Other?	☐
	If Other please specify.		A new long term collaboration between the Trust and the Breast Pathology Research Group at University of Nottingham			

2.2.1	What data will be processed?					
	Personal Data:					
	Forename	☐	Surname	☐	Age	☒
	DOB	☐	Gender	☒	Address	☐
	Post Code	☐	NHS No	☐	Hospital No	☐
	Other unique identifier (please specify)		Lab number, Referral route, Menopausal status, Date of diagnosis, Family history of cancer			
	Sensitive Personal Data (special categories):					
	Children					☐
	Vulnerable groups					☐
	Racial or ethnic origin					☐
	Political opinion					☐
	Religious Belief					☐
	Trade Union Membership					☐
	Physical or mental health or condition					☒
	Sexual Health					☐
	Criminal offence data					☐

	Other data (please specify)	Pseudonymised number

2.2.2	Is the data?					
	Identifiable?	☐	Pseudonymised?	☒	Anonymised?	☐

2.3	Is the data required to perform the specified task?	
	Y/N	Please justify response **Yes or No**
	Y	The research projects cannot be performed without access to samples and linked metadata. The number of data items proposed is limited to those essential for such studies, based on our long-term experience in research (>30 years) and from peer-reviewed publications (~700) in the field. Details of the items needed for the patient database are given in Appendix 1 together with justification for inclusion where necessary and how the data fields will be adapted for use in the Pseudonymised Database: DPIA%20Appendix%201%20-%20Fields%20 Developing diagnostic and prognostic tools for breast cancer is most effective when done against large sets of data. There is no other effective way to achieve this objective. Data has been minimised to the fewest essential fields required to meet this purpose. Modifications of the data to decrease the risk of re-identification, and the risk assessment are summarised in Appendix 2. DPIA%20Appendix%202%20-%20Data%20r
2.3.1	How will you collect, use, store and delete data?	
	Our data team who are responsible for collecting and overseeing the use of data comprises the following: **Data Management Team** This team will have access to the Trust's data systems and patient information. They are responsible for pseudonymising the database. This team creates and holds the link key. • Medical laboratory assistant (to be appointed as part of the project team at the Trust and funded by University of Nottingham) - TBC • SFH IT contact – TBC	

- Christopher Nolan – University of Nottingham Technician (holds Trust Honorary contract)
- Lavanya Sattianarayanin – University of Nottingham Technician (holds Trust Honorary contract)

Data Collection Team

This team will access the Trust's systems to collect and quality checks the relevant patient data. They do not have access to the pseudonymisation code or the link.

- the Trust and/or University employees with Trust Honorary Contract

Data Access Committee

The Data Access Committee considers and authorises requests to access the data from the pseudonymised database.

- Prof Emad Rakha (University of Nottingham)
- Dr Gill (the Trust)
- Jennifer Baldwin (University of Nottingham)
- Christopher Nolan (University of Nottingham)
- Lavanya Sattianarayanin (University of Nottingham)

Data Manager

Oversees the whole process & is the project principal investigator.

- Prof Emad Rakha

Collect

Data will be collected by our Data Collection Team who will have NHS contracts, and who will access patient records to collect the relevant patient, treatment and outcome data.

Personal identifiable data fields such as patient pathology lab number, hospital number, and date of birth will be only used during the data collection/update phase of the database to ensure data accuracy and validity during the process of collection (ie. ensuring the Data Collection Team (University of Nottingham and the Trust) is collecting the required data for each patient and that the patient record is located correctly). However, this data is not needed in the research and will not be transferred to the pseudonymised database or shared with the research team.

The Data Collection Team (University of Nottingham and the Trust) will work with the dedicated NHS staff in the Trust's Pathology Department.

Dates of particular types of treatment or outcome events will be kept in the restricted-access database. These dates will be not be used in the final database released to researchers, as shown in the 'Fields Required' document (Appendix 1), instead they will be grouped into 'categories' to further reduce risk of re-

identification.

DPIA%20Appendix%201%20-%20Fields%20

To minimise the risk of re-identification of any patient, we have modified it as shown in Appendix 2.

DPIA%20Appendix%202%20-%20Data%20r

Data, including personal identifiers, will be collected and stored in a Microsoft Excel spread sheet, kept in a controlled-access secure encrypted folder on the Trust's network drives. This is accessible by the Data Collection Team (University of Nottingham and the Trust) and remains owned by the Trust.

The data will be pseudonymised by the Data Management Team (designated individuals from the Trust and University of Nottingham with Trust Honorary contracts) and the pseudonymised database will be constructed when collection of data items is complete. Therefore, no researcher will have access to patient identifiable information.

The de-identification code will be double coded; the first code is a 4 digit randomly selected code and the second will be generated from a hash, then saving the data in a separate folder with the personal identifiers removed.

The pseudonymised data will be deposited by the Data Management Team into a separate folder within the confines of the Trust's secure IT network. The Data Management Team will be the only personnel with access to the link between personal identifiers and the pseudonymisation code, it will not be available to the primary clinical care or research teams.

Pseudonymised data will not include specific dates.

The pseudonymised code will be the same for data and tissue for a particular patient.

Pseudonymised data will be transferred to the University via secure encrypted email from NHS accounts.

Use

The data will be linked to research-generated data. The latter will be generated from the researchers work on the sample tissue. The link between data and tissue is needed for:

1. Selection of subgroups/cohort for specific studies.
2. Training and validation of digital pathology algorithms
3. Running the required statistical analyses for research.

We are not intending to generate any unique genetic data in our research projects that could potentially lead to patients' identification.

The data is being used for the purpose of developing and testing diagnostic and prognostic tools, which is most effective when done against large data sets. Tissue based research will also be performed using linked metadata.

The Breast Pathology Research Group (BPRG) is involved in processing pseudonymised clinical data, and any data released to researchers will be modified to further reduce the risk of re-identification. Modification of the data and the associated risk assessment is detailed in Appendix 2.

DPIA%20Appendix%202%20-%20Data%20r

Pseudonymised data may be shared with collaborators and other parties with particular expertise or facilities for analysis. Data sharing for any particular project will be approved by the Data Access Committee (representatives from Breast Pathology Research Group (BPRG) and the Trust) after reviewing the relevant application documents and requests. The Data Access Committee is:

- Prof Emad Rakha (UoN)
- Dr Gill (SFH)
- Jennifer Baldwin (UoN)
- Christopher Nolan (UoN)
- Lavanya Sattianarayanin (UoN)

The Data Management team will release the pseudonymised data to approved researchers to achieve the research goal of developing and validating diagnostic and prognostic tools for refining breast cancer management. This is identified as a task in the public interest (Article 6 (1) (e)) and for ensuring high standards of quality and safety of care (Article 9 (2) (I)). It will also be used in projects to obtain research grants to support the ongoing collaboration and sustainability of the research activity at University of Nottingham and the Trust for the ultimate benefits of breast cancer patients.

Store

The full data set including the patient-identifiable data and links to pseudonymisation codes will be held within the Trust's NHS secure IT network. Only the Data Management Team has access to this.

Pseudonymised processed data will be transferred via secure NHS email (or any other secure method advised by the Trust) to University of Nottingham where it will be held in a controlled-access folder on the secure University of Nottingham password protected IT system, in accordance with the University of Nottingham Information Security Policy.

The NHS Digital Data Security Centre has reviewed the Data Security and

Protection Toolkit for University of Nottingham – EE133856-RGD - the latest review date was March 2020 with 19/20 Standards Met.

The Data Flow diagram (Appendix 3) illustrates data locations.

Appendix 3 - Data Flow Diagram.pdf

The encrypted spreadsheet with the pseudonymised data will be stored in a secure, limited access folder within the University of Nottingham firewall.

Access to the folder will be granted to authorised researchers/students by their Principle Investigator/Supervisor and the Data Access Committee, and is controlled by the Data Management Team (University of Nottingham and the Trust).

The Data Management Team creates encrypted subfolders for each researcher/student containing the pseudonymised data required for their particular study and gives them individual access details to this specific folder/file only.

The researchers/students have access only to the pseudonymised data of the subset of cases that they are interested in and working on, based on their research question and hypothesis. They do not have access the whole dataset.

The whole pseudonymised dataset will only be accessed by the Data Management Team. All data files and subfiles are stored within a secure area within the University of Nottingham network firewall which is owned by and accessible only to the Breast Pathology Research Group with appropriate support from the University of Nottingham IT staff.

The administration rights will be controlled by the Data Management Team and authorised by the principal investigator.

Prior to providing access to any of these folders to our researchers/students all users will carry out the proper training on data security and usage and are asked to sign Terms and Conditions statement that clearly states that they are not allowed to copy or download any of the data file outside the University of Nottingham secure area, and that any breach will be taken very seriously.

We will set a mechanism with our University of Nottingham IT to allow our Data Management Team to log and record access to the data folders and flag any attempt to data downloading, copying and/or transferring outside the University of Nottingham secure area.

Delete

When a researcher leaves the group, his/her access to the University IT systems, and hence the data folder, will be disabled. This is standard university policy.

Research generated data from this project will be held in the University secure folder for 15 years to allow building large set of research biomarker data that will help the clinical and research breast cancer communities and will be a core resource to apply for grants to fund our long term collaboration between both

	parties Projects involving external collaborators will be subject to appropriate processing limitations outlined in the legal contract and data sharing agreement which will stipulate the destruction of data once the project is completed and an appropriate time has been allowed for processing and publishing outcomes. Involvement will be subject to the University of Nottingham Third Party Access policy.
2.3.2	What is the source of the data? (i.e. from data subject, system or other third party)
	Data will be collected entirely from the Trust's clinical records and patient notes. Data fields required are located in different Trust systems such as PAS, WinPath, NotIS, Chemocare and Mosaic (relevant systems to be finalised with the Pathology IT team). No data collection from prospective patients is planned. Data collection is from historical retrospective archived cases diagnosed between 2000-2015. Patients will not be contacted at any stage of this project.
2.3.3	How much data will you be collecting and using?
	This data covers Sherwood Forest Hospitals Trust breast disease patients and involves data belonging to patients presented to the Trust with breast disease from 1st January 2000 to 31st December 2015. Collectively, it consists of data relating to approximately 6,000 patients derived from medical records of the Trust, covering their region.
2.3.4	How often? (for example monthly, weekly)
	From our long experience with research and data collection, the process of collecting the required data from ~ 6000 samples will take approximately 12 months. After that, accessing the data systems will be sporadic (if needed) to check the validity/accuracy of the collected data or to update the outcome data.
2.3.5	How long will you keep it?  NHSX_Records_Mana gement_Code_of_Prac
	The duration of database data processing will be 5 years. The pseudonymised database will be used for up to 15 years, enhanced and enriched with research data. The processing – ie gathering the data from patient records (together the 6000 cases) will be for up to 5 years which is the length of the REC application. When we have gathered the data and it has been pseudonymised and transferred to Nottingham we will maintain it for up to 15 years, developing and enhancing it with further research data. This is the independent research database. If we need to use it for longer we will apply for an extension of the REC. None of this data is fed back to the Trust's patient records, it is pseudonymised research data.

	Funding will be sought to further extend the duration of the database to be used in future ethically approved research projects if required.
2.3.6	Where will the data be stored? i.e. Medway, Shared Drive, offsite storage
	The patient - identifiable data will be held within the Trust's NHS Trust secure IT network. Pseudonymised, numerically encoded data will be held in a controlled-access folder on the secure University of Nottingham password protected IT system with full backup, in accordance with the University of Nottingham Information Security Policy and the University of Nottingham IT Network policy.
2.3.7	How many individuals are affected?
	6000 cases
2.3.8	What geographical area does it cover?
	All patients who were treated at the Trust between 1st January 2000 and 31st December 2015 who are predominantly from Mansfield, Ashfield, Newark, Sherwood and parts of Derbyshire and Lincolnshire.

2.4	Who are the Organisations involved in processing (sharing) the data?	
	Organisations Name	Data Controller or Data Processor *The **Data Controller** is a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.* *The **Data Processor**, in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.*
	Sherwood Forest Hospitals NHS Foundation Trust	Data Controller
	Breast Pathology Research Group, University of Nottingham	Data Processor

2.5	If we have identified a supplier in 2.4, the following questions for 2.5 and 2.6 will need to be answered by the supplier and the Trust	
	Y/N	**If yes the third party will need to complete the following assessment. This will need to be provided in addition to**

		the completion of this proforma. An example of a completed assessment is also provided below  NHIS - Supplier Assurance Framework  Supplier Assurance Framework - Example
		 NHIS%20Supplier%20Assurance%20Frame

2.5.1	Please describe access and controls in place (Account Management SOP to be created)
	Data on the Trust's IT system is encrypted. Patient identifiable data will not be moved outside the Trust's IT network. Pseudonymised data will be transferred to the University via secure and encrypted email. Access to the Trust's data systems will be restricted to personnel employed by the Trust or University of Nottingham personnel holding Trust Honorary contracts (research passports) who are subject to standard Trust data management and Information Governance controls. Data collection and management on the Trust system will be carried out using NHS managed PCs and/or laptops in secure locations. Files linking personal data with pseudonymisation number will be kept within the Trust's IT system and further protected by password-only access, managed by the Pathology IT team. The data kept within the Trust's IT system will be controlled by the Trust's IT department and subject to standard access controls managed by the Trust. Data kept on the University system will be subject to University access controls as outlined in the University of Nottingham Information Security Policy. Access to the University folder containing the information will be controlled by the chief investigator and password-protected. The University has MFA for off-site access to its IT systems. All access to pseudonymised data will be through the University network. Also see NHS Digital Data Security Protection review (DSP Toolkit Review for University of Nottingham EE133856-RGD – 19/20

	Standards Met) Pseudonymised data released to University of Nottingham researchers will be stored in the protected folder for use is not allowed to be downloaded onto personal laptops or PCs. Prior to providing access to any of the data subsets to our researchers/students, all users will carry out the proper training on data security and usage. They will be asked to sign Terms and Conditions that clearly states that they are not allowed to copy or download any of the data file outside the University of Nottingham secure area and any breach will be taken very seriously. We will develop a mechanism with our University of Nottingham IT colleagues to allow our Data Management Team to log and record access to the data folders and flag any attempt to download data, copying and/or transferring outside the University of Nottingham secure area.		
2.5.2	Please provide a copy of the contract in place		
	We are currently applying for REC and CAG approval. This DPIA is required as part of the Confidentiality Advisory Group (CAG) application. Once REC and Confidentiality Advisory Group (CAG) approval are granted, a collaboration agreement will be drawn up between the University of Nottingham and Sherwood Forest Hospitals Trust.		
2.5.3	Have arrangements for retention and destruction been included in the contract when the service/contract expires?		
	This will be built into the collaboration agreement. This is not a specific project agreement but it aims for ongoing research collaborations involving multiple students. We request access to the Trust's patient data for an initial 5 years in order to identify and build the cohort of 6000 cases. We will use the pseudonymised database for research purposes for 15 years as outlined in the REC application.		
2.5.4	Is the supplier registered with the ICO? Please check the register	Yes	No
		X	
2.5.5	Has the supplier received ICO	Yes	No

	Enforcement? Please check the register		X
2.5.6	Has the supplier received ICO Decision Notice? Please check the register	Yes	No
		ICO Decision Notice - UoN - fs50732288.pdf ICO Decision Notice - UoN - fs50803451.pdf ICO Decistion Notice - UoN - fs50718980.pdf Please note: The decision notices are in relation to Freedom of Information Requests	
2.5.7	Has the supplier received an ICO Audit? Please check the register	Yes	No
			X

2.5.8	Has the supplier completed a Data Security and Protection Toolkit, please check the register and provide the following details	Completed: Yes/No	Date submitted	Standard Met/Not Met
		Yes - EE133856-RGD	02.03.2020	19/20 Standards Met

2.5.9	Can the supplier demonstrate compliance with any of the following standards? If YES please provide further information e.g. date achieved and a copy of the certificates		
		Yes	No
	Cyber Essentials Plus		Part of the University's infrastructure is Cyber Essentials accredited but this accreditation does not at this time cover our entire

			network, this may be reviewed in future.
	ISO 15489 Records Management		No
	ISO 27001 Information Security Standards		Our O365 environment is ISO accredited however our entire network has not been through accreditation
	ISO 9001 Quality Management Systems		No

2.5.10	Is the data held outside of the UK ie Europe, USA, Ireland? If yes please include the country	
	Yes	No
		X
	If yes we need to seek assurance that the data will continue to flow post Brexit 31.12.2020, provide further detail below from the supplier	
	N/A	
2.6	Will this information be shared outside the organisations listed above?	
	Y/N	if answered **Yes** please describe organisation/s and geographic location
	Y	Identifiable data will not be moved outside of the confines of the Trust's NHS IT system. Pseudonymised data may be shared from University of Nottingham with external collaborators for specialised analysis which cannot be done 'in-house', e.g. statistical analysis, development of machine-learning codes. The sharing will be secured by encrypting the spreadsheet and sending the data through by secure email. The password for the shared files will be shared with collaborators in a separate email, not included with the data files.
2.7	Does the work involve employing contractors external to the Organisation?	
	Y/N	If **Yes**, provide a copy of the confidentiality agreement or contract?
	Y	Our Data Management Team and Data Collection Team are employed by University of Nottingham but we are also

		applying for Trust NHS Honorary Contracts for them.				
2.8	Has a data flow mapping exercise been undertaken?					
	Y/N	If **Yes**, please provide a copy here. Have the information flows and assets that are identified within this DPIA been added to your departmental information flow map and asset register? If **No**, please complete – Section 3				
	Y	The Data Flow Diagram (Appendix 3) can be seen here: Appendix 3 - Data Flow Diagram.pdf This is to be added to the Data Management Plan (DMP) which is logged centrally at the University.				
2.9	What format is the data?					
	Electronic	☒	Paper	☐	Other (Please describe)	Click here to enter text.

2.10	Is there an ability to audit access to the information?	
	Y/N	Please describe if answered **Yes.** If **NO** what contingencies are in place to prevent misuse?
	Y	Only the Data Management Team and Data Collection Team, who hold NHS Honorary Contracts, will have access to the Trust's IT system. They are bound by NHS/Trust regulations and monitoring regarding access to, and use of, patient information systems. Employees holding Research Passports are subject to enhanced DBS checks and a code of conduct relating to the use of patient data. Alongside any sanctions that the Trust may apply, breaches of confidentiality or misuse of NHS systems will be dealt with as Gross Misdemeanours within the University of Nottingham disciplinary policy. All other users – researchers within the Breast Pathology Research Group (BPRG), students etc. will all need to request access to the data via the Data Access Committee. A database of applications records every request.

2.11	Does the system involve new links with personal data held in other systems or have existing links been significantly changed?

	Y/N	Please describe if answered **Yes**
	N	

2.12	How will the information be kept up to date and checked for accuracy and completeness? (data quality) How will you ensure data minimisation?
	This is a one-time collection of data of patients presenting with breast cancer and its precursor lesions at the Sherwood Forest Hospitals NHS Trust. between 1st January 2000 - 31st December 2015. It includes clinical and outcome data gleaned from the Trust's patient systems. All records will be checked against the National Opt Out System before collection begins. We are mindful of data minimisation throughout the project and will ensure we will only collection the information required for our study (see Appendix 2 – Risk Assessment).  DPIA%20Appendix%202%20-%20Data% Specific personal data fields are required for ensuring accuracy of data collection - that we are locating the correct patient record – for recording treatment and outcome information, and for quality checking of the data. This includes patient name, Hospital number, and date of birth. These personal data fields will be only used during the data collection/update phase of the database. Similarly, dates of particular types of treatment or outcome events will be kept in the restricted-access database. These dates will be not be used in the final database released to researchers, as shown in the 'Fields Required' document (Appendix 1), instead they will be grouped into 'categories' to further reduce risk of re-identification.  DPIA%20Appendix%201%20-%20Fields%20 When considering requests for tissue samples and related data for individual research projects, the Data Access Committee will take into account the aims of the project when determining what data fields are required, releasing only those deemed essential.
2.13	Who will have access to the information? (list individuals or staff groups)
	Data Management Team This team will have access to the Trust's data systems and patient information. They are responsible for pseudonymising the database. This

	team creates and holds the link key. • medical laboratory assistant (to be appointed as part of the project team at the Trust) - TBC • Trust IT contact – TBC • Christopher Nolan – University of Nottingham Technician, Breast Pathology Research Group (BPRG) with Trust Honorary Contract • Lavanya Sattianarayanin – University of Nottingham Technician, Breast Pathology Research Group (BPRG) with Trust Honorary Contract **Data Collection Team** This team will access the Trust's systems to collect and QC the relevant patient data. They do not have access to the pseudonymisation code or the link. • the Trust and/or University employees with Trust Honorary Contract **Data Access Committee** The Data Access Committee considers requests to access the data from the pseudonymised database. • Prof Emad Rakha (University of Nottingham) • Dr Gill (the Trust) • Jennifer Baldwin (University of Nottingham) • Christopher Nolan (University of Nottingham) • Lavanya Sattianarayanin (University of Nottingham) **Data Manager** Oversees the whole process & is the project principal investigator. • Prof Emad Rakha (University of Nottingham)

2.14	What security measures have been implemented to secure access?	
	Active Directory (Window's username and password)	☐
	Username and password	☒
	Smartcard	☐
	Key locked filing cabinet/room	☐

	Hard/soft Token (VPN) Access	☒
	Restricted Access to Network Files (shared drive)	☒
	Has information been anonymised?	☐
	Has information been pseudonymised?	☒
	Is information fully identifiable?	☐
	Other (provide detail below)	☐

2.15	Will the data be stored on Trust servers	
	Yes	No
	Full data on Trust server	Pseudonymised data on University of Nottingham server

2.16	Please state by which method the information will be transferred?			
	Email (not NHS.net)	☐	NHS.net	☒
	Website Access (internet or intranet)	☐	Wireless Network (Wi-Fi)	☐
	Secure Courier	☐	Staff delivered by hand	☐
	Post (internal)	☐	Post (external)	☐
	Telephone	☐	SMS	☐
	Fax	☐	Other (please specify below)	☐

2.17	Are disaster recovery and business contingency plans in place for the information? What types of backups are undertaken i.e. full, differential or incremental?	
	Y/N	Please describe if answered **Yes.** Please state why not if response is **No.**
	Y	In line with the university policy on IT Network Security, regular and full data back-ups are taken.
2.18	Has staff training been proposed or undertaken and did this include confidentiality and security topics areas?	
	Y/N	Please describe if answered **Yes**
	Y	Data security training is mandatory for all University of Nottingham employees. Compulsory refresher training is regularly required. Any Breast Pathology Research Group (BPRG) staff member who has an honorary contract will undertake the Trust's mandatory data security training, with the annual follow-ups.
2.19	Will reports be produced?	
	Will reports contain personal/sensitive personal or business confidential information?	Any reports will be in the format of scientific publications in journals and will not reference any personal information.
	Who will be able to run reports?	
	Who will receive the reports and will they be published?	
2.20	If this new/revised function should stop, are there plans in place for how the information will be **retained / archived/ transferred or disposed of?**	
	Y/N	Please describe if answered **Yes.** Please state why not if response is **No.**
	Y	Pseudonymised information will be retained on the University of Nottingham secure IT system.

2.21	Is consent required for processing of personal data?	
	Y/N	Please describe if answered **Yes**
	N	We are applying to Confidentiality Advisory Group (CAG) as the historical cases are not consented.
		If **No**, list the reason for not gaining consent e.g. relying on an existing agreement, consent is implied, the project has s251 approval or other legal basis?
		We are using historical data which, at the time it was gathered, was not consented for research purposes. The University of Nottingham is applying for section 251 authorisation (April 2021) to undertake this retrospective research study on 6000 Trust patients.
2.22	Will individuals be informed about the proposed uses and share of their personal data?	
	Y/N	Please describe if answered **Yes.** Please state why not if response is **No.**
	N	We will not directly contact individuals.
2.23	Is there a process in place to remove personal data if data subject refuses/removes consent	
	Y/N	Please describe if answered **Yes.** Please state why not if response is **No.**
	Y	Records will be checked against the National Data Opt-Out Scheme.
2.24	How much control will they have? Would they expect you to use their data in this way?	
	Y/N	Please describe if answered **Yes.** Please state why not if response is **No.**
	Y	The use of patient data in research is essential for identification of novel biomarkers, improving the quality of diagnosis, prediction of outcome and refining management decisions for future patients. This will improve outcome in terms of survival time, quality of life and cost savings for the

		NHS. This project is based on using tissue surplus to diagnosis together with a limited, pseudonymised dataset. This work has been discussed with members of the public, including patients, at a number of Nottingham-based public engagement events: within the Nottingham University 'Life Cycle' fundraising campaign and the Nottingham Breast Cancer Research Centre (NBCRC) outreach project. No concerns over the responsible use of samples and data by the research teams have been raised at these events; on the contrary, we have received a great deal of positive feedback and public support for the research effort. More recently, we have involved the Nottingham University Hospitals NHS Trust Patient and Public Involvement and Engagement team in explaining our purpose to the public, with favourable initial responses from the breast cancer patient groups to our information leaflet which has been distributed across their memberships (see Appendix 4). Appendix 4 - Information Leaflet - L We are currently investigating similar approaches with the Trust's Patient and Public Involvement and Engagement contact, Fiona Haynes. In addition, there is a national interest in maximising the benefit of patients' data by increasing the number of cases included in research projects, and several national and European initiatives have started in the UK and Europe to build up data lakes that contain data on hundreds of thousands of patients. Consenting individual patients may not be possible with such large-scale studies so the NHS has introduced the opt out scheme for the use of patients' data in research that supports the move toward public interest in a way that maximises the use of such data, but respects patients' rights to withdraw from contribution. The following Trust procedure will be used to check whether a patient has opted-out of the use of their data for research purposes at the

		start of the project. Their wishes will be respected.  National Data Opt-out for Clinical Audits and All NHS numbers MUST be checked using the trusts 'National Data Opt-out checker' (https://sfhinformationhub.nnotts.nhs.uk/MESH/import_check. The checker requires you to input the research and innovation project reference number you are checking data for and then you will be required to enter the NHS numbers you wish to use for the research. For projects using more than 50 NHS numbers please use the following link: https://sfhinformationhub.nnotts.nhs.uk/ADHOCS/Request.
2.25	Are arrangements in place for recognising and responding to requests for access to personal data?	
	Y/N	Please describe if answered **Yes.** Please state why not if response is **No.**
	Y	The Trust has a Data Protection Policy and Procedure in place for responding to subject access requests.
2.26	Who are the Information Asset Owner(s) and Administrator(s)?	
	IAO	Professor Emad Rakha (University of Nottingham) Elaine Torr (the Trust)
	IAA	Jennifer Baldwin (University of Nottingham) Christopher Nolan (University of Nottingham) Clair Sleney (the Trust)
	System Administrators	Data Collection Team (University of Nottingham) Clair Sleney (the Trust)
2.27	How is the data secured in transit? Eg encryption, port control number	
	Data is encrypted before transfer and is transferred from the Trust to University of Nottingham via secure NHS email.	

<table>
<tr><td>2.28</td><td colspan="2">Has the impact to other NHIS systems/processes been considered and appropriate SBU’s consulted and in particular technical security?</td></tr>
<tr><td rowspan="3"></td><td>Y/N</td><td>Please describe if answered Yes.
Please state what checks were undertaken if response is answered No.</td></tr>
<tr><td>Y</td><td>We will consult with the pathology IT team to ensure we can have the read-only access we require to the patient systems.</td></tr>
<tr><td rowspan="3">2.29</td><td colspan="2">Are there any current issues of public concern that you should factor in?</td></tr>
<tr><td>Y/N</td><td>Please describe if answered Yes.</td></tr>
<tr><td>N</td><td></td></tr>
<tr><td rowspan="2">2.30</td><td colspan="2">What do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?</td></tr>
<tr><td colspan="2">This project will support breast cancer research in the Trust and University of Nottingham aimed at developing robust diagnostic and prognostic tools to help pathologists in accurately diagnosing breast cancer with improved efficiency. The intended benefits are for both service users and the providers of those services.

• diagnostic/prognostic biomarker discovery
• developing tools for slide image analysis
• developing automated systems for improving quality and throughput in diagnostic histopathology.</td></tr>
<tr><td rowspan="2">2.31</td><td colspan="2">Consider how to consult with relevant stakeholders:

• Describe when and how you will seek individuals’ views – or justify why it’s not appropriate to do so.
• Who else do you need to involve within your organisation?
• Do you need to ask your processors to assist?</td></tr>
<tr><td colspan="2">Communication plans will be developed with the Trust’s Public Patient Information and Engagement Department to ensure that lay representatives and community members are aware of the work being undertaken, the proposed outcome, and how this will provide a better healthcare service to the breast cancer patients in improving diagnosis and treatment outcome. This is particularly important due to the possible negative perceptions of artificial intelligence and its place in health care services.

Longer term, as joint project bids are prepared between the Trust and Breast Pathology Research Group (BPRG) we will consult with the PPI group on</td></tr>
</table>

	projects, gain their feedback and invite them as lay representatives to join our steering committees. In addition, we will seek advice and support from the Trust's IT and the IG teams to ensure that data management is secure, robust and meets the highest standards of governance, and that we have access to the relevant systems as required.

2.32	What is your lawful basis for processing? (please see Appendix 10 Information Sharing Protocol for further information). **Consent is usually the last basis to rely on** **Legal basis: patients** **Personal data i.e. name, address** 6(1)(a) the patient has given consent 6(1)(c) necessary for legal obligations 6(1)(e) public interest or public duty 6(3) the above supported by Member State law (UK legislation as applicable to circumstances) **Sensitive personal data (special category)** 9(2)(a) the patient has given explicit consent 9(2)(c) processing for 'vital interests' (safety, safeguarding, public safety, etc.) 9(2)(h) allows processing for the provision of healthcare (direct care) or the management of healthcare systems (invoice validation, commissioner reporting, quality audits – essentially, mandated activity). 9(2)(i) allows processing for "ensuring high standards of quality and safety of health care." – which would cover research, audit, service improvement and addressing public health/inequalities. 9(2)(j) (together with Article 89 and relevant recitals) relates to archiving, statistical analysis and research. **Legal basis: staff** – please review Appendix 10 Information Sharing Protocol for further information).
	We are using historical data which, at the time it was gathered, was not consented

	for research purposes. The University of Nottingham is applying for section 251 authorisation (April 2021) to undertake this retrospective research study on 6000 Trust patients.
2.33	What information will you give individuals about the processing? (This information will be added to the Trust's Patient Privacy Notice and Staff Privacy Notice by the Information Governance Team)
	We will issue our information leaflet for the Trust's patients (similar to Appendix 8) explaining in detail: • The purpose and need for this research • How it will benefit patients in the future, and the NHS • What sort of data is being collected and how it will be used • How data will be secured and patients' interests protected. • How patients may opt out of involvement. It will be made clear that their treatment is in no way affected by refusal of consent. Patients' rights to confidentiality will be protected by pseudonymisation of their data and measures to prevent re-identification by any means. Sharing of data with researchers will require ethical approval and any collaborations with third parties will be defined by legally binding contracts that limit use of data. Requests for access to the anonymised data will be reviewed and authorised by the Data Access Committee. Data Access Committee is: • Prof Emad Rakha (UoN) • Dr Gill (SFH) • Jennifer Baldwin (UoN) • Christopher Nolan (UoN) • Lavanya Sattianarayanin (UoN)

2.34	What measures do you take to ensure processors comply?
	The processes outlined throughout the DPIA relating to training, agreements and

	approved access will ensure compliance. We will also have legal contracts, MTA and DTA agreements in place with relevant parties.
2.35	How will you prevent function creep? Manage lifecycle of system/process
	Use of the pseudonymised data will be in ethically approved projects and the release of the pseudonymised data will be regulated by the Data Access Committee. Data Access Committee is: • Prof Emad Rakha (UoN) • Dr Gill (SFH) • Jennifer Baldwin (UoN) • Christopher Nolan (UoN) • Lavanya Sattianarayanin (UoN) Sharing of data with other research groups or collaborators will be subject to legally binding and enforceable Data Processing and Data Transfer Agreements drawn up by qualified professionals.

Stage - 3 Risk Template

For advice on completing this Risk Template please contact the Risk & Assurance Manager on x6326

What is the activity that is being risk assessed?

Data collection for the Prognostic and Molecular Classification of Breast Cancer for Personalised Therapy project

Completed by: Jenny Baldwin Role: Research Projects Officer, Breast Pathology Research Group, University of Nottingham Date completed:

Risk description What event could happen which would impact on the activity? What would cause it to happen? What would the consequence be?	**Primary controls** What is in place now to prevent the risk from occurring or to act as a contingency if it does occur?	**Current risk**			**Gaps in control** If the risk is not controlled to an acceptable level, what are the issues that need to be addressed?	**Acceptable risk**			**Mitigating actions required** What needs to be done to reduce the risk to an acceptable level?
		Consequence	**Likelihood**	**Rating (C x L)**		**Consequence**	**Likelihood**	**Rating (C x L)**	
Unintended release of data set beyond project recipient.	Agreement between Breast Pathology Research Group (BPRG), the Trust's IT and IG regarding pseudonymisation process and secure storage of data. Data Management and Collection Teams to hold Trust Honorary Contracts/Research passports. Application process to request use of the data and tissue to be developed, with representation from the	4	2	8	Enforcement actions by the ICO against the Trust, University of Nottingham and individuals, possibly including fines and criminal prosecution. Damage to reputations of University of Nottingham, the Trust, NHS and employees.	4	1	4	Data sets are subject to comprehensive arrangements for secure storage and transfer. Contracts and data sharing agreements to be in place forbidding the sharing of these data beyond the intended recipient. Data recipient due diligence identifies no concerns. Contracts in place to ensure ongoing compliance for data use and sharing.

Risk description What event could happen which would impact on the activity? What would cause it to happen? What would the consequence be?	**Primary controls** What is in place now to prevent the risk from occurring or to act as a contingency if it does occur?	**Current risk**			**Gaps in control** If the risk is not controlled to an acceptable level, what are the issues that need to be addressed?	**Acceptable risk**			**Mitigating actions required** What needs to be done to reduce the risk to an acceptable level?
		Consequence	**Likelihood**	**Rating (C x L)**		**Consequence**	**Likelihood**	**Rating (C x L)**	
	Trust and Breast Pathology Research Group (BPRG).								Data set has been pseudonymised to a very high level to minimise the impact to data subjects should an inadvertent disclosure or loss of data occur.
Failure of the de-identification of data process	Pseudonymisation is a manual process and may be subject to human error. Pseudonymised data sets will be checked by two people before release to researchers.	4	2	8	Enforcement actions by the ICO against the Trust and individuals, possibly including fines and criminal prosecution. Damage to reputations of University of Nottingham, the Trust, NHS and employees.	4	1	4	Pseudonymised data sets will be checked by two people before release to researchers.
University of Nottingham misuses the Trust's personal data, eg. by trying to re-identify individual's	The data will be pseudonymised to a level whereby it is highly improbable that a single individual may be re-identified from the data set without the linking key. Only the Data Management Team has access to the Trust's IT system and their usage is monitored as per the Trust's IT security policies.	4	2	8	Enforcement actions by the ICO against the Trust and individuals, possibly including fines and criminal prosecution. Damage to reputations of University of Nottingham, the Trust, NHS and employees.	4	1	4	At data collection stage the data subjects are identifiable through the linking mechanism; the linking table is held securely and separately within the confines of a separate folder controlled by the Trust's IT system and away from the data itself. Once pseudonymised, all data is held and transferred securely. Researchers are

Risk description What event could happen which would impact on the activity? What would cause it to happen? What would the consequence be?	**Primary controls** What is in place now to prevent the risk from occurring or to act as a contingency if it does occur?	**Current risk**			**Gaps in control** If the risk is not controlled to an acceptable level, what are the issues that need to be addressed?	**Acceptable risk**			**Mitigating actions required** What needs to be done to reduce the risk to an acceptable level?
		Consequence	**Likelihood**	**Rating (C x L)**		**Consequence**	**Likelihood**	**Rating (C x L)**	
									prohibited from attempting any re-identification and bound by contract to inform the Trust should the data be found to be identifiable.
Infringement of data subject rights and freedoms	The processing of this data is lawful and proportionate and meets the requirements of UK GDPR.	4	2	4	Enforcement actions by the ICO against the Trust and individuals, possibly including fines and criminal prosecution. Damage to reputations of University of Nottingham, the Trust, NHS and employees.	4	1	4	Confidentiality Advisory Group (CAG) approval is currently being applied for. Strong technical controls are in place to protect these data and the applied de-identification limits risk to data subject privacy.
The University of Nottingham is applying for section 251 authorisation (April 2021) to undertake this retrospective research study on 6000 Trust patients. If the application is rejected the research study would not have a legal basis in order to proceed.	Currently applying to the Confidentiality Advisory Group (CAG) for section 251 approval	4	2	4	Enforcement actions by the ICO against the Trust and individuals, possibly including fines and criminal prosecution. Damage to reputations of University of Nottingham, the Trust, NHS and employees.	4	1	4	Confidentiality Advisory Group (CAG) approval is currently being applied for.

Risk Scoring Matrix.pdf

Stage – 4 Legal Compliance

Compliance to be determined by IG team from the responses provided in the previous stages, delete as appropriate:

Data Protection Act 2018	Compliance and Comment
Principle 1 – Personal data shall be processed fairly and lawfully and, in a transparent manner	Lawfulness • We have identified an appropriate lawful basis (or bases) for our processing. • We are processing special category data and have identified a condition for processing this type of data. • We don't do anything generally unlawful with personal data. Fairness • We have considered how the processing may affect the individuals concerned and can justify any adverse impact. • We only handle people's data in ways they would reasonably expect, or we can explain why any unexpected processing is justified. • We do not deceive or mislead people when we collect their personal data. Transparency • We are open and honest, and comply with the transparency obligations of the right to be informed.
Principle 2 – Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes	• We have clearly identified our purpose or purposes for processing. • We have documented those purposes. • We include details of our purposes in our privacy information for individuals. • We regularly review our processing and, where necessary, update our documentation and our privacy information for individuals. • If we plan to use personal data for a new purpose other than a legal obligation or function set out in law, we check that this is compatible with our original purpose or we get specific consent for the new purpose.

Principle 3 – Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed	• We only collect personal data we actually need for our specified purposes. • We have sufficient personal data to properly fulfil those purposes.
Principle 4 – Personal data shall be Accurate and, where necessary, kept up to date, having regard to the purposes for which they are processed, are erased or rectified without delay	• We ensure the accuracy of any personal data we create. • We have appropriate processes in place to check the accuracy of the data we collect, and we record the source of that data. • We have a process in place to identify when we need to keep the data updated to properly fulfil our purpose, and we update it as necessary. • If we need to keep a record of a mistake, we clearly identify it as a mistake. • Our records clearly identify any matters of opinion, and where appropriate whose opinion it is and any relevant changes to the underlying facts. • We comply with the individual's right to rectification and carefully consider any challenges to the accuracy of the personal data. • As a matter of good practice, we keep a note of any challenges to the accuracy of the personal data
Principle 5 – Kept no longer than is necessary	• We know what personal data we hold and why we need it. • We carefully consider and can justify how long we keep personal data. • We have a policy with standard retention periods, however due to the Goddard Inquiry no destruction or deletion of patient records is to take place until further notice.
Principle 6 – Appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage	• We undertake an analysis of the risks presented by our processing, and use this to assess the appropriate level of security we need to put in place. • We have an information security policy (or equivalent) and take steps to make sure the policy is implemented. We

	have put in place technical controls such as those specified by established frameworks like Cyber Essentials. • We use encryption. • We understand the requirements of confidentiality, integrity and availability for the personal data we process. • We make sure that we can restore access to personal data in the event of any incidents, such as by establishing an appropriate backup process. • We conduct regular testing and reviews of our measures to ensure they remain effective, and act on the results of those tests where they highlight areas for improvement. • We implement measures that adhere to an approved code of conduct or certification mechanism. • We ensure that any data processor we use also implements appropriate technical and organisational measures.