Project title:	Airways Trial
Reference number:	
Implementing organisation:	Sherwood Forest Hospitals NHS Foundation Trust
Key contacts involved in the DPIA (name and job title)	Terri-Ann Sewell – Research Operations Manager Alison Steel - Head of Research and Innovation Gina Robinson, Information Security Officer
Information Asset Owner (name and job title)	Alison Steel, Head of Research and Innovation
Information Asset Administrator (name and job title)	Terri-Ann Sewell, Research Operations Manager

Step 1 – What is the aim of the project being undertaken

Q1	**Project description: Describe in sufficient detail for the project to be understood**	A multi-centre, open-label, pragmatic, individually randomised, parallel group, superiority trial and economic evaluation to determine the clinical and cost effectiveness of a supraglottic airway (SGA) versus tracheal intubation (TI) during in-hospital cardiac arrest (IHCA). The trial will include an internal pilot to confirm feasibility.

Risk Template

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

Completed by: Terri-Ann Sewell Role: Research Operations Manager Date completed: 22nd February 2023

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** Consequence	Likelihood	Rating (C x L)	**Gaps in control** If the risk is not controlled to an acceptable level, what are the issues that need to be addressed?	**Acceptable risk** Consequence	Likelihood	Rating (C x L)	**Mitigating actions required** What needs to be done to reduce the risk to an acceptable level?
Loss of system access due to connection failure or server failure either via NHIS or 3rd party supplier. Loss of data leading to an inability to complete the research, This could result in the service being disrupted or unavailable.	All data processed will be stored on University of Warwick servers, which comply with the University Back Up policy. Contingency plans and security measures are in place for threats to the IT infrastructure that contain the servers. Hard copies of trial data not backed up electronically will be kept to a minimum and imputed onto electronic systems as soon as possible. Data Protection and Management procedures and technical controls ensure	2	1	2		2	1	2	

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)**	
	passwords are changed, and they conform to good password practice to minimise the risk of hacking attempts.								
Loss of system data due to connection failure or server failure by third party supplier. This could result in the service being disrupted or unavailable.	All data processed will be stored on University of Warwick servers, which comply with the University Back Up policy. Contingency plans and security measures are in place for threats to the IT infrastructure that contain the servers. Hard copies of trial data not backed up electronically will be kept to a	2	1	2		2	1	2	

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)**	
	minimum and imputed onto electronic systems as soon as possible. Data Protection and Management procedures and technical controls ensure passwords are changed, and they conform to good password practice to minimise the risk of hacking attempts.								
Data is accessed inappropriately due to lack of access controls. Movers and leavers access not removed. Data is inappropriately processed and/or disclosed	Username and password controls in place. Access is managed within the Trust's research team. Account Management and access procedure to be audited on a regular basis. Appropriate access according to role. IG Training in place.	2	2	4		2	2	**4**	

Risk Scoring Matrix.pdf

Step 8 – Legal compliance

To be amended by Information Governance from the responses provided in the previous stages.

UK General Data Protection Regulation 2018	Compliance
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. • We periodically review the data we hold, and delete anything we don't need.
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 three Inquiries including the Goddard Inquiry, no destruction or deletion of patient records is to take place until further notice. • We clearly identify any personal data that we need to keep for public interest archiving, scientific or historical research, or statistical purposes.

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. • When deciding what measures to implement, we take account of the state of the art and costs of implementation • We have an information security policy and take steps to make sure the policy is implemented. • When deciding what measures to implement, we take account of the state of the art and costs of implementation • We make sure that we regularly review our information security policies and measures and, where necessary, improve them. • We have assessed what we need to do by considering the security outcomes we want to achieve. • We have put in place technical controls such as those specified by established frameworks like Cyber Essentials. • We understand that we may also need to put other technical measures in place depending on our circumstances and the type of personal data we process. • We use encryption and/or pseudonymisation where it is appropriate to do so. • 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. • Where appropriate, 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.

Principle 7 – Accountability principle	• We take responsibility for complying with the UK GDPR, at the highest management level and throughout our organisation. • We keep evidence of the steps we take to comply with the UK GDPR. • We put in place appropriate technical and organisational measures, such as: ☐ adopting and implementing data protection policies (where proportionate); ☐ taking a 'data protection by design and default' approach - putting appropriate data protection measures in place throughout the entire lifecycle of our processing operations; ☐ putting written contracts in place with organisations that process personal data on our behalf; ☐ maintaining documentation of our processing activities; ☐ implementing appropriate security measures; ☐ recording and, where necessary, reporting personal data breaches; ☐ carrying out data protection impact assessments for uses of personal data that are likely to result in high risk to individuals' interests; ☐ appointed a data protection officer; and ☐ adhering to relevant codes of conduct and signing up to certification schemes (where possible). ☐ We review and update our accountability measures at appropriate intervals.

Step 9 - Assessment Summary

To be completed by Information Governance.

Outcome of Data Protection Impact Assessment	
Project is not recommended to proceed, as significant risks have been identified.	☐
Project to proceed once identified risks have been mitigated as agreed.	☐
Project has met required legislative compliance and poses no significant risks. No further action required.	☒

Summary of Data Protection Impact Assessment; including legislative compliance and identified risks	
Legislative Compliance:	**Suggested text, remove, amend as necessary.** Article 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. Article 9(2)(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes
Summary of Risks	**Suggested text, remove, amend as necessary.** Cyber security, loss of data, inappropriate access to data, inability to access data and Information Asset Management.
Identified risks	
The risk	**Mitigation**
Loss of system access	Full system back-up process in place
Loss of system data	Full system back-up process in place
Data is accessed inappropriately	Individual username and passwords are provided.

Recommendations for Action

Summary of recommendations (amend/delete as necessary)		
Recommendations	**Recommendations**	**Agreed deadline for action**
Information Asset Administrators to ensure Warwick is added to the information asset register and data flows are mapped and recorded	IAO/IAA	1st April 2023
Ensure business continuity plans are in place	IAO/IAA	Annual
Account management Standard Operating Procedure generated and implemented, routine audit to take place	IAO/IAA	Bi-annual audit

Project signoff

	Name	Job Title	Date
Information Asset Owner*	Alison Steel	Head of Research and Innovation	1st March 2023
Data Protection Officer	Jacquie Widdowson	Information Governance Manager	1st March 2023
Senior Information Risk Owner	Shirley Higginbotham	Director of Corporate Affairs	26th April 2023
Caldicott Guardian	David Selwyn	Medical Director	26th April 2023
Patient safety[1]			

The Data Protection Impact Assessment must be reviewed and approved by the Information Asset Owner, Data Protection Officer, Senior Information Risk Owner and Caldicott Guardian. Approval does not close the data protection risks related to this project.

*It is important that the risks and the original scope of the project are reviewed on a regular basis to ensure any new confidentiality, integrity or availability risks are identified, documented, and mitigated wherever possible. All amendments must be approved following the approvals process.

[1] DCB0129: Clinical Risk Management: its Application in the Manufacture of Health IT Systems - NHS Digital