Information Governance Checklist for the introduction a of new database*:

Part 1: Concept stage		
Title	**Management (M) Aortic Graft Infection (AGI) Collaboration (C) service evaluation database pilot – MAGIC DATABASE**	
Clinical site contact:	Dr. Nicholas Price (GSTT)	
Sponsor:		
PRIMARY SITE (GSTT) IT Contact:	Bolaji Coker (Biomedical Research Centre KCL)	
Date:		
Please indicate which applies *As part of implementing this project more than one of the list may apply*	Implementation of a new database	**x**
	Introduction of new process	
	Setting up of new contract	
Date approved		

	Checklist Questions	Response	For IG use only: Additional information/ Actions
Project Outline			
1	Please provide a detailed outline of the project	This service evaluation is part of a national aortic endograft infection collaboration initially involving 5 vascular surgery centres in the UK and in partnership with the British Society of Antimicrobial Chemotherapy and The Vascular Society of Great Britain. Data collection will be performed prospectively by five English NHS vascular surgery centres: Leeds General Infirmary, University Hospital South Manchester, Birmingham Heartlands Hospital, The Royal Free Hospital, and Guys' & St Thomas' Hospital. All centres already routinely employ a multidisciplinary team involving Infectious Diseases Physicians/ Microbiologists and Vascular Surgeons in the case management of endovascular graft infections. Data relating to the initial clinical presentation, diagnostic methods, surgical intervention, antimicrobial management and specific outcomes of AGI patients will be entered into a secure pseudo-anonymised on-line database (http://www.gsttbrc.com/magic/) developed at the National Institute of Health Research (NIHR) Biomedical Research Centre (BRC) at Guy's and St Thomas' NHS Foundation Trust and Kings College London (http://www.guysandstthomasbrc.nihr.ac.uk). The data will be used for the following: 1) To derive combinations of diagnostic criteria - related to outcome data - that validate a robust, practical working AGI case definition. This is also a pivotal starting point for producing clinical guidance and enabling meaningful comparison between scientific studies. 2) To promote heightened awareness and early identification of AGI by characterising initial presenting clinical features more precisely. 3) In the absence of high quality research evidence, to derive recommendations regarding the utility of various radiological and microbiological methods/ techniques in the diagnosis of AGI. 4) Similarly, by relating interventions with outcome, to assist in making recommendations about optimal antimicrobial and surgical treatments. 5) To expand the evidence base and share experience of AGI diagnosis and management by developing a national registry/ database through inclusion of other centres with a commitment to a similar multidisciplinary clinical approach. 6) Highlight key questions about the effectiveness of various diagnostic and treatment strategies that should be addressed by research studies beyond the scope of this present work.	
2	Have you funding in place to proceed with this project?	Group Funding has been secured. There is no individual funding necessary at this time	

3	For new applications/software/databases Do you have approval from the IT Project Group/ Design Authority	Not Applicable. Design Authority and deployment has been reviewed and managed at GSTT through IT support services.	
Personal identifiable data - data protection			
4	Will you be using/holding personal identifiable information? *Such as name, address, dob, NHS number, hospital number, photographs, CCTV, NINO*	Personal identifiable information (hospital number, DOB, initials, and microbiology laboratory specimen numbers) will only be held at the local level as per clinical need. All information placed in the database will be pseudoanonymised prior to entry. Age will be used as a non-identifiable proxy for date of birth. Data at the local level will be held in concordance with local and national NHS guidelines with respect to the Data Protection Act 1998 and Caldicott Guidelines.	
5	If yes: please specify if this is patient, staff or other personal data.	N/A	
6	Will you also be holding sensitive personal data (such as ethnicity, religious beliefs, health etc)?	No sensitive personal data will be held in the database.	
7	Will you be using patient identifiable data for any other purpose other than healthcare e.g. research or training? If yes – have you put in place a process to obtain the patients consent for this use?	The project has been designated a national service evaluation by the NRES therefore patient consent is not required.	
8	Will any data be processed/shared outside the UK? If yes – please identify the countries	No	
9	Are procedures in place to provide access to records on receipt of a subject access request?	Not applicable	
10	Do you intend to send direct marketing messages by electronic means such as by telephone, fax, email, text message and picture (including video) message or by using an automated calling system?	No	
Other types of data			

11	Other than the personal data described in question 3 above please outline the type of data to be held/ processed.	Baseline clinical information (comorbidities, severity of illness), infection-related and microbiological parameters, outcome data.	
12	What format will this data be held in e.g. electronic, paper?	Paper records kept for internal purposes. Electronic records are kept for analysis and shared with the national group of collaborators.	
13	Where will this data be held (off site/on site, server, website, mobile device, third party)? If any data is held off site please let us know the location	GSTT has purchased a licence for MedSciNet Clinical Trial Database Framework and pays a yearly fee for Operation, Maintenance and Support. GSTT use the service in order to develop Clinical databases used within GSTT. Data is entered into a secure electronic web-based database at http://www.gsttbrc.com/magic/ which is both HSCIC Information Governance Toolkit compliant (level 2 or above) and ISO 27001/27002:2005 certified Generated applications and the databases reside on servers in Amsterdam, provided by the company Interoute, acting as a subcontractor of MedSciNet U.K. Ltd. Interoute is accredited according to ISO 27001 and the contract between MedSciNet AB (the mother company in Sweden) and Interoute contains all necessary clauses regarding standard NHS Terms and conditions including information governance, security, confidentiality and support.	
14	For what purpose will the data be held – clinical care, service/organisation, business, research or audit?	Service evaluation	
Access controls			
15	What access controls will be introduced to control who has access to the information? Please identify the controls that will be used e.g. password, user id etc	Access to the data will be restricted to collaborators and controlled by user id and password using a role based system.	

16	Please identify the staff roles who will be involved in using this system/process.	Clinicians, nurses, statisticians, data manager.	
Third party contractor			
17	Is a service being contracted from a third party?	Yes, see section 13	
18	If Yes: will they be processing Trust Data, if yes please outline what they will be doing	The system will be processing only pseudoanonymised data entered into the web-based database.	
19	If Yes: will they be providing a service e.g. supplying an application/software system?	yes, see section 13	
20	Will they require remote access to the Trust systems?	No	
Stakeholder analysis			
21	Provide a broad list of any departments or organisations that may have an interest in, a role to play in delivering, or be affected by the project.	**GSTT Directorate of Infection** (Primary Service Evaluation Administration Site) **GSTT BRC** (IT services, database and data management support) **Leeds General Infirmary** (Patient Enrolling Site) **University Hospital South Manchester** (Patient Enrolling Site) **Birmingham Heartlands Hospital** (Patient Enrolling Site) **The Royal Free Hospital** (Patient Enrolling Site) **Guys' & St Thomas' Hospital** (Patient Enrolling Site)	
Information sharing			
22	Will you be sharing patient identifiable data with an external organisation?	Patient identifiable data will not be shared between partner NHS organisations. Only pseudoanonymised data will be housed within the database with each organization able to access their own data and the central site, GSTT, able to access all the data.	
23	If Yes: Who will you be sharing data with?	Not Applicable	

24	How will this information be shared with the external organisation e.g. email/ fax/ post/ internet connection/ telephone?	Not Applicable	
Information Security			

25	What type of security controls will be in place to prevent unauthorised access, loss or damage to any personal identifiable information? Please identify what these controls are?	Users will only be able to access the online database with their username and password. These usernames, with the required access rights, will be provided by the central centre, GSTT. The only other staff that will have access to the data will be GSTT BRC data management services team and the web hosting team managing the physical servers and backups in compliance with ISO 270001. All transmission of data from the web frontend to the database backend is done through Secure Socket layers (SSL). Only users advised by the Principal Investigator at each centre are given usernames. Initially, when a user is first given a username they are a given a temporary password and forced to change it when they first login. In general, the management of the database will be in compliance with the GSTT data protection policy per Appendix 2 Item 7.2: The measures that the Trust has in place must ensure a level of security appropriate to the nature of the data and must consider the harm that might result from disclosure. Therefore the Trust must seek to ensure its compliance with ISO17799: which governs personnel measures; physical security; environmental security; document and media protection; hardware security; software security; data security; back-up; maintenance; contingency planning; and security awareness. This policy can be provided to all stakeholders on request	

26	Will you be using any mobile devices? If yes – please identify the type of devices & identify whether they will be encrypted	No.	
Business Continuity			
27	Will this system/process be incorporated into the department's business continuity plan?	No. Business continuity activities will be done by the GSTT data management services team and the web hosting team.	
Records management			
28	Is this information covered by the Trust Retention and Destruction schedule? If no – add appropriate retention period to local retention and destruction schedule?	No. However the data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes. With specific reference to the retention, archiving and destruction of the service database, the database will be held for a period of 5 years from the formal closure of enrolment.	
29	If appropriate have any medical records forms been approved by the MRRG?	Not applicable	
NHS Number			
30	Will this system act as a master index to flow Patient Identifiable Data and NHS Numbers to other systems?	Not applicable.	
31	Will the system be used to produce hard-copy outputs containing Patient Identifiable Data? This includes patient appointment letters, reports shared externally with other organisations / individuals.	No	
32	Will the system need to transfer information between organisations?	No	
33	Will the NHS Number, as a national identifier, ever be required to be stored against Patient Identifiable Data in the system for e.g. audit purposes?	The NHS number is not required.	

Part 2
Data Quality

34	Are national or locally defined data standards (format and content) being used wherever possible? (*please refer to the appropriate Data Set Change Notification)*	Yes	
35	Where different systems are recording the same data, are processes in place to ensure there are no inconsistencies between them?	Not applicable as data is only recorded once.	
36	Confirm that a process for identifying and recording of changes to stored data is in place.	Yes. All changes to the database are logged	
Information Security			
37	Have processes been considered to protect information and physical assets from accidental loss, destruction or damage such as through flood or power failure or theft?	Yes. Databases are hosted by Interoute holding an ISO27001 certification ensuring physical security: • Auxiliary power through UPS and diesel generator; • Physical surveillance with video and infra-red cameras; • Climate control system is used for temperature and humidity monitoring; • Burglary alarm; • ESD protected elevated floor. Grounding according to IBM standard; • A pass card and PIN code is required to access the building; • Fire extinguishing system is based on aragonite gas, fire is detected by smoke and heat sensors.	
38	Are controls in place to protect the system from malicious software?	Yes. The system uses Enterprise Symantec endpoint protection tools.	
39	Are appropriate and secure backup processes in place?	Yes. Data is backed up daily, with a window of 7 days, on the server. A differential backup is also done daily and a full backup done at the weekend with a window of 30 days.	
40	Are procedures and controls in place to ensure that only authorised personnel may carry out software and hardware maintenance?	Yes. Only staff of the GSTT BRC data management service can carry out software modifications. Only staff for the web hosting infrastructure can carry out hardware maintenance.	

Access controls			
41	Are passwords enforced for access to the system?	Yes	
42	What is the password complexity for the system e.g. how many characters/alpha/numerical/symbols	Password should be at least 4 and no more than 20 characters in length.	
43	Will users have access to all information held on the system or access based on their roles?	No, users can only access their own data	
44	Are there access profiles in place for the system – if yes please provide information as to what these are and who is responsible for approving the access profiles	Yes. The system has roles for users (has read write access to all data for their centre), unit administrator (has read write access to all data for their centre and can add and disable other users for that centre), monitor (has only read access to all data, for one or more centres, and can raise queries in the data and lock them), principal (has read write access to all data at the centre, can electronically sign all patients once they have been locked by the monitor role, and can unlock data), global admin (has full rights over system by being able to add and disable users, extract data, and unlock records). The data controller for the database is Dr Nicholas Price.	
45	Who is responsible for approving system access	Senior Data manager at GSTT	
46	Is there an audit trail available of who has been accessing the system? If yes – what audit logs are available	Yes. Audit logs available include details of all successful and failed logins, details of all changes to the data (insertion and updates) – deletions are not allowed, and details of all menu actions.	
47	Is there an inbuilt time out after a period of inactive use?	Yes	
Capacity Planning: New systems or major changes to existing systems will require additional resources, including:			
48	Has the capacity (bandwidth and storage space) of the existing network to cope with the introduction of this system been considered as part of the implementation planning process?	Not applicable as web-based system hosted by GSTT	
49	Have implications for technical support, training, maintenance, replacement costs, human resources and other implications all been taken into consideration?	Not applicable as web-based system hosted by GSTT	

50	Have additional physical resources such as furniture, paper supplies, training materials and material storage cabinets been considered?	Not applicable as web-based system hosted by GSTT	
Test System Development (Solution Build) Systems in development or under test can cause problems to operational systems or live data, and should therefore be separated until ready for introduction as an operational system.			
51	Is there a separate environment for testing purpose?	Yes	
52	Confirm that operational data is not being used on test systems. Test data should be created or the use of live data justified.	Operational data is not used in the test environment. All data used for testing and training is fictitious.	
53	Are documented procedures in place governing the transfer of software from development to operational status (see system acceptance questions below)?	Yes. All procedure documentation is held with the Senior Data manager at GSTT and can be reviewed on request.	
54	Confirm that test systems are subject to the same access and security controls as operational data.	The test environment is subject to the same access and security controls as the operational data.	
Documented Operating Procedures (Required Prior to Deployment) Documented operating procedures should be made available for all users of systems, as part of user training. It is essential that the procedures are kept up to date, to reflect any changes to software/hardware or working methods. System administrators and technical support personnel will also need access to more detailed operating procedures to carry out their roles. Procedures should include:			
55	Have information processing and handling instructions been produced?	Not applicable as web-based system hosted by GSTT	
56	Have instructions for handling operational errors been produced?	Not applicable as web-based system hosted by GSTT	
57	Have support contacts for operational or technical difficulties been identified?	Not applicable as web-based system hosted by GSTT	
57	Have instructions for handling output and media, including the disposal of confidential waste and failed jobs been produced?	Not applicable as web-based system hosted by GSTT	
59	Will activity audit and log data be collected for this system? If yes, have procedures been produced?	Not applicable as web-based system hosted by GSTT	
Change Management (CM) (Required Prior to Deployment) System software, hardware and operating procedures are subject to regular change. It is essential that any changes are subject to a strict CM regime to ensure that all changes are controlled and approved. Failure to do this can result in system faults or failures. Formal documented Request for Change procedure should be used.			

60	Confirm that change control management process are in place and will be applied to this system	Not applicable as web-based system hosted by GSTT	
System Acceptance This is the last stage of development where a system is moved through to operations. All IT systems should follow the Transition to Live Checklist Procedure and also answer the following questions:			
61	Have error recovery and restart procedures been documented?	Not applicable as web-based system hosted by GSTT	
62	Have routine operating procedures been prepared and tested?	Not applicable as web-based system hosted by GSTT	
63	Have security controls been agreed?	Not applicable as web-based system hosted by GSTT	
64	Have any manual procedures been documented?	Not applicable as web-based system hosted by GSTT	
65	Have system dependencies been documented and assessed and added to the information asset register under the entry for this system?	Not applicable as web-based system hosted by GSTT	
66	Have business continuity plans been created and tested?	Not applicable as web-based system hosted by GSTT	
67	Have disaster recovery plans for the hardware and infrastructure components been created and tested?	Not applicable as web-based system hosted by GSTT	
68	Is evidence (through testing and calculations) that the new systems will not adversely affect existing operational systems available?	Not applicable as web-based system hosted by GSTT	
69	Has training in the use of the system for user and technical support been carried out?	Not applicable as web-based system hosted by GSTT	
70	Has there been user involvement at all stages of system development to ensure the system is as intuitive as possible.	Not applicable as web-based system hosted by GSTT	
Managing clinical risk Please complete the questions below if you are implementing a clinical system, for further information please refer to DSCN 14/2009 & DSCN 18/2009. In developing and deploying any software locally, (i) do you have in place, and (ii) have you implemented, through appropriate testing, a process (where applicable) for -			
71	Ensuring that when data is transferred FROM the Trust's IT systems to your own that the data is attributed to the correct patient	Not applicable	

72	Ensuring that when data is transferred TO the Trust's IT systems from your own that the data is attributed to the correct patient	Not applicable		
73	Ensuring that where data mapping occurs between elements in the Trust's systems and your own that these are properly attributed and represented	Not applicable		
74	Ensuring that your software displays information consistent with the work practices of the Trust e.g. Trust guidelines , protocols etc	Not applicable		
75	Ensuring that your software displays data in a manner which is safe and consistent with that expected by your staff in the light of any relevant training that they may have received	Not applicable		
76	Ensuring that your software is used by your staff in the way intended and that any controls within your system are not subverted	Not applicable		
Criticality of the system Please indicate how critical the system is, this decision should be considered with no controls in place. If the system is critical to the Trust then an unavailability risk assessment is completed that outlines the controls that are in place.				
77	In discussion with the IAO how critical is the loss of this system/application: for each time period specified, please indicate if the loss of the system is a low, medium or high risk	<4 hour	low	If a critical asset level 1-3 complete an unavailability risk assessment with the department
		4-12 hours	low	
		12-24 hours	low	
		24 plus	low	
		Not discussed		
System security template				
78	Please complete a system security template for any application/system that contains personal identifiable data see System-level Security Policy for details	Not applicable as web-based system hosted at GSTT with no personal identifiable data		