Nottinghamshire Health Informatics Service
Transforming care through technology

NHS
Sherwood Forest Hospitals
NHS Foundation Trust

Privacy & Security Impact Assessment

Title	Ref number
Audit Management and Tracking (AMaT) to manage Clinical Audit and Ward Assurance (Perfect Ward) process	

PAGE	1-16	1-17	1 - 17	1-19	1-19	1-20	1-21
ISSUE	V 0.3	V 0.4	V3.0	V4.0	V5.0	V5.1	V5.2
DATE	Sept 2015	Sept 2015	Dec 2015	June 2017	Nov 2017	June 2018	October 2018

Introduction

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

Nottinghamshire Health Informatics Service, who are hosted by Sherwood Forest Hospitals NHS Foundation Trust, provides information Communication and Technology services. Nottinghamshire Health Informatics Service is responsible for implementation of Information Communication and Technology systems and provision of the network infrastructure.

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.

Privacy & Security Impact Assessments 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 Privacy & Security Impact Assessment has a responsibility to ensure that Patient Safety, Technical Security and Quality Impact Assessments are considered, in line with NHIS and the Trust procedure.

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 Privacy & Security Impact Assessment (Full) **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 Corporate Governance	✓	

OR

If a Privacy & Security Impact Assessment (Full) **IS** required **Activity**	**Implementer**	**Governance**
Complete Stage 2 – Privacy & Security 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 Corporate Governance	✓	

This document is intended to be used by both NHIS and SFHFT jointly to complete the Privacy Impact Assessment (PIA) process. The *Governance* section will be completed by SFHFT IG Team with support from the relevant NHIS specialist teams as applicable.

Project Details

Project Title:	**AMAT to manage Clinical Audit and Ward Assurance (Perfect Ward) process**

Project Description: ***Describe in sufficient detail for the proposal to be understood***
The project will replace the current Meridian system for processing Clinical Audit and Ward Assurance with Audit Management And Tracking (AMaT) system provided by Meantime IT. These two markers of safety and quality are stored in different modules that are not widely visible and accessible to all staff at SFH, making it harder to share 'quality' knowledge. The Audit contract is due to end in March 2020 and the Ward Assurance contract ends in August 2020. This one system will specifically replace the current 3 Audit processes – data trackers, registration process and the data analysis. This knowledge platform is a 'game changer' in terms of organisational memory of improvement and audit work, and will reduce immediate costs in terms of the comparative price of the two systems, as well as releasing longer term benefits in avoiding repeat activities where not indicated i.e. re-audits when previous audits have been done. Supplier – Meantime IT Software supplied by Meantime IT – AMaT (Audit Management And Tracking) IT support provided by Rackspace to Meantime IT

Overview of the proposal: ***What the project aims to achieve***
Please see above for project aims

Implementing Organisation:	Sherwood Forest Hospitals NHS Foundation Trust

Staff involved in PIA assessment (Include Email Address):	Barbara Jurczyk – Barbara.Jurczyk@nhs.net Corinne Kitchen – Corinne.Kitchen@nhs.net Louise Randle – Louise.Randle@nhs.net Ann Fewtrell – Ann.Fewtrell@nhs.net Ceri Feltbower – Ceri.Feltbower@nhs.net Beth Proud – Bethany.Proud2@nhs.net

	Craig Short – Craig.Short@nhs.net

Key Stakeholders/Customers:	All SFH staff

Project Sign Off

	Name	Job Title	Organisation	Date
Information Asset Owner	Emma Challons,	Director of Culture and Improvement	Sherwood Forest Hospitals NHS Foundation Trust	**19th May 2020**
Information Asset Administrator	Ceri Feltbower	Associate Director of Service Improvement	Sherwood Forest Hospitals NHS Foundation Trust	**19th May 2020**
Information Governance	Gina Robinson	Information Security Officer	Sherwood Forest Hospitals NHS Foundation Trust	11th March 2020
Third Party Representative *(someone aware of project and appropriate level of responsibility)*	Steve Parker		Meantime IT	**28th February 2020**
Caldicott Sign Off	Shirley Higginbotham	Director of Corporate Affairs	Sherwood Forest Hospitals NHS Foundation Trust	**3rd June 2020**
SIRO Sign Off	Paul Robinson	Chief Financial Officer	Sherwood Forest Hospitals NHS Foundation Trust	**21st May 2020**
Data Protection Officer	Jacqueline Widdowson	Information Governance Officer/ DPO	Sherwood Forest Hospitals NHS Foundation Trust	**12th May 2020**

Assessment Summary

To be completed by Information Governance / NHIS

Outcome of Privacy & Security 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 no significant risks. No further action required.	☒

Summary of Privacy & Security Impact Assessment; including legislative compliance and identified risks:
Summary: AMaT outsource their IT to Rackspace Limited The use of Javascript which is not recommended by NHS Digital **Risks to SFHFT**: Cyber Security risk

Recommendations for Action

Summary of Identified Recommendations? :

AMaT undertake due diligence with all their suppliers as part of their ISO 27001 accreditation. Rackspace Limited are ISO 27001 accredited.	**Recommendation Owner:** Gina Robinson	**Agreed Deadline for action** Completed 5th March
AMaT requires the use of Javascript for the software to work effectively. Cyber Security, NHIS have identified that this is a minor risk and that AMaT/Rackspace Limited are providing a secure environment and that there are mitigations in place ie penetration testing, that prevents Javascript behaving in a bad way. AMaT is cloud-based and accessed by a web browser, there would be no changes required locally, or to any infrastructure, and the Javascript is self-contained to the website. No impact is expected to any other systems.	**NHIS**	Approved 11th March 2020

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 PIA will be undertaken on a case-by-case basis by NHIS / SFHT IG.

Q	Screening question	Y/N	Justification for response
1	Will the project involve the collection of information about individuals?	Y	Audit data will be the main focus of the tool and information will be collected along audit guidelines
2	Will the project compel individuals	N	

Q	Screening question	Y/N	Justification for response
	to provide information about themselves?		
3	Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	N	
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?	N	
5	Are there processes in place to ensure data is relevant, accurate and up-to-date?	Y	Audit team will consistently manage this system which will include ensuring data is relevant, accurate and up-to-date
6	Are there security arrangements in place while the information is held?	Y	Rackspace provide IT support to Meantime IT. Both organisations are ISO 27001 certified
7	Does the project involve using new technology to the organisation?	N	
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	
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 tool is not a patient facing Health IT system and a patient safety case/compliance with DCB0129 is not needed.
10	Is a Quality Impact/Technical Security Review required?	Y	Completed by NHIS Technical and Cyber Security March 2020. AMaT outsource their IT to Rackspace Limited The use of Javascript which is not recommended by NHS Digital. Further detail in stage 4.

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

Stage 2 – Data Protection and Security Impact Assessment

2.1	What is the change					
	New purpose?	☐	Revised/changed?	☐	Other?	☒
	If Other please specify.		Replacement system			

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)		Forename and surname for staff only			
	Sensitive Persona Data (special categories):					
	Children					x
	Vulnerable groups					x
	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)					

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	Data used for clinical audit

2.3.1	How will you collect, use, store and delete data?
	A member of staff registers for an audit and this is approved by the audit team and the member of staff inputs data into the database, this is then analysed by the database to enable the staff member to draw conclusions. Data can only be deleted by the supplier at the request of the audit team

2.3.2	What is the source of the data? (ie from data subject or other third party)
	From medical records and other electronic clinical systems (Medway, ICE, Orion, CRIS, NerveCentre, and Bluespier) held in the hospital. This data will be collected by staff within the Trust undertaking audit and then this will be inputted into the AMaT software.

2.3.3	How much data will you be collecting and using?
	Typical audit cycle around the year is approx. 200 audits. In addition to this the tool will be collecting service improvement projects.

2.3.4	How often? (for example monthly, weekly)
	Used on a daily basis

2.3.5	How long will you keep it? https://www.sfh-tr.nhs.uk/media/1974/records-management-code-of-practice-health-and-social-care-2016.pdf
	5 years. AMaT will delete data at the request of the audit team.

2.3.6	Where will the data be stored? i.e. Medway, Shared Drive
	The data/system is hosted in a private cloud environment at Rackspace in London. The system will be accessible via a web browser and using the NHS Digital Cloud Risk Assessment this has scored as a Class 1 - All organisations are expected to be comfortable operating services at this level.  health_and_social_care_data_risk_model (

2.3.7	How many individuals are affected?
	All staff

2.3.8	What geographical area does it cover?
	All geographical areas covered by the Trust

2.4	Who are the Organisations involved in processing (sharing) the data?	
	Organisations Name:	*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.*
	Data Controller	Sherwood Forest Hospitals NHS Foundation Trust
	Data Processor	Meantime IT 2.1, Riverside Business Park, Natland Rd, Kendal LA9 7SX

2.5	Does a third party have access to existing network or systems (remote or onsite)?	
	Y	**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 Supplier Assurance Framework AMAT 20(
		2 risks identified in stage 4, outsourcing IT and the use of Javascript

2.5.1	Please describe access and controls in place
	The audit team will control which members of staff have access to the system and will remove the access once no longer required. Quarterly reviews of access to be undertaken by the Trust

2.5.2	Please provide a copy of the contract in place
	NHS Standard Contract will be drawn up by procurement when the system is signed off during May 2020.

2.5.3	Have arrangements for retention and destruction been included in the contract when the service/contract expires?	
	Once the contract expires the Trust will follow the Transfer of Data Policy. Previous audit data will be transferred from Meridian to AMaT	
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	Meantime IT and Rackspace will have access to the data. Meantime IT 2.1, Riverside Business Park, Natland Rd, Kendal LA9 7SX

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?
	N	

2.8	Has a data flow mapping exercise been undertaken?

	YES	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  Audit Data Flow Map 2020.xlsm and asset register? If **No**, please complete – Section 3

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	AMaT offers the ability to audit who/when logged in and who entered data. This can be done at any point in time if needed

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?
	The audit team will undertake daily checks of the information on the system and ensure its accurate and complete

2.13	Who will have access to the information? (list individuals or staff groups)
	Audit team – all access Improvement team – all access

	Other SFH staff – as and when required for an individual audit. AMaT gives different levels of access to different staff groups and this is controlled by the audit team.

2.14	What security measures have been implemented to secure access?	
	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 any information be sent offsite? – i.e. outside of the organisation and its computer network	
	Y/N	Please describe if answered **Yes**
	Y	Data will be stored on Rackspace servers in London. Rackspace are ISO 27001 certified and provide IT services to Meantime IT ISO 27001 certified who own the AMaT software
	Are you transferring personal data to a country or territory outside of the EEA?	
	Y/N	Please identify data sets and destinations if answered **Yes**
	N	

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)	☒
	Data is accessed via a web browser. NHIS aware.			

2.17	Are disaster recovery and business contingency plans in place for the information?	
	Y/N	Please describe if answered **Yes.** Please state why not if response is **No.**
	Y	The audit team does not have a current business continuity plan but will contact Mark Stone to discuss this.

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	Yes – all staff have access to audit training which includes how to use the database. All staff undertakes IG training on an annual basis.

2.19	Will reports be produced?	
	Will reports contain personal/sensitive personal or business confidential information?	The AMAT system has the ability to publish reports regarding stage/progress of audit. The audit topic may include

		personal data (eg grouping patients by age) so the report would include anonymised data relating to a group of patients. There would be NO individual data in any report.
	Who will be able to run reports?	Staff undertaking audits and the audit team
	Who will receive the reports and will they be published?	Staff undertaking audits, the audit team, the lead sponsor and divisional mangers

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	The contract will include an agreement regarding archived data being available to SFH if the system is no longer in place. The Trust will follow the Transfer of Data Policy

2.21	Will explicit consent be obtained for processing of personal data?	
	Y/N	Please describe if answered **Yes**
	N	
		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?
		Consent is not required The following legal basis apply: 6(1)(e) public interest or public duty; 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.

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.**

	Y	Our privacy notice includes the 'your NHS Data Matters' standard wording which describes that patient data is used for 'improving the quality and standards of care provided' https://www.sfh-tr.nhs.uk/about-us/contact-us/your-personal-information-data-protection-act-privacy-notice/

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	The audit team will instruct Meantime IT to delete personal data. Confirmation of destruction will be provided to the Trust.

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	Local audits are not in scope of the national data-opt-out programme and patient consent for local audits is not required by law.

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 will follow the Data Protection, Confidentiality and Disclosure Policy and Procedure.

2.26	Who are the Information Asset Owner(s) and Administrator(s)?	
	IAO	Emma Challons
	IAA	Ceri Feltbower

2.27	Has the impact to other NHIS systems/processes been considered and appropriate SBU's consulted and in particular technical security?

	Y/N	Please describe if answered **Yes.** Please state what checks were undertaken if response is answered **No.**
	Y	The software (AMaT) is cloud-based and accessed via a web browser. NHIS have confirmed that there are no changes to be required locally. No impact is expected to any other systems.

2.28	Are there any current issues of public concern that you should factor in?	
	Y/N	Please describe if answered **Yes.**
	N	

2.29	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?
	This one system will specifically replace the current 3 Audit processes – data trackers, registration process and the data analysis. This knowledge platform is a 'game changer' in terms of organisational memory of improvement and audit work, and will reduce immediate costs in terms of the comparative price of the two systems, as well as releasing longer term benefits in avoiding repeat activities where not indicated i.e. re-audits when previous audits have been done

2.30	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?
	We have already consulted with relevant stakeholders at meetings across SFH and we have held 3 demonstrations of the system at SFH to which relevant stakeholders have attended and the feedback has been positive

2.31	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).
	6(1)(e) public interest or public duty; 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.

2.32	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)
	Our privacy notice includes the 'your NHS Data Matters' standard wording which describes that patient data is used for 'improving the quality and standards of care provided' https://www.sfh-tr.nhs.uk/about-us/contact-us/your-personal-information-data-protection-act-privacy-notice/

2.33	What measures do you take to ensure processors comply?
	NHS Standard Contract Terms and Conditions

2.34	How will you prevent function creep?
	The database will only allow for restricted data inputting in relation to audit and improvement this will therefore prevent function creep from occurring . DPIA to be reviewed 6 months after implementation.

Stage - 3 Work Flow Mapping

Please note: Have the information flows and assets that are identified within this DPIA been added to your departmental information flow map and asset register?

Yes.

Stage - 4 Identified Risks and Mitigating Action

Risk:	L	I	Max Risk Rating *	Solution Options(s):	Approved Solution:	Approved by:	L	I	Mitigated Risk Rating *	Mitigating Officer	Date to be completed:
AMaT outsource their IT to Rackspace Limited	3	3	9	AMaT undertake due diligence with all their suppliers as part of their ISO 27001 accreditation. Rackspace Limited are ISO 27001 accredited. https://dab35129f0361dca3159-2fe04d8054667ffada6c4002813eccf0.ssl.cf1.rackcdn.com/downloads/pdfs/Rackspace-ISO27001-Presentation-Cert.pdf	Yes	Gina Robinson, Information Security Officer	2	2	4		Completed 5th March 2020
The use of Javascript which is not recommended by NHS Digital https://digital.nhs.uk/about-nhs-digital/standards-for-web-products/web-products-	4	3	12	AMaT requires the use of Javascript for the software to work effectively. Cyber Security, NHIS have identified that this is a minor risk and that AMaT/Rackspace Limited are providing a secure environment and that there are mitigations in place ie penetration testing, that prevents Javascript behaving in a bad way. AMaT is cloud-based and accessed by a web browser, there would be no changes required locally, or to any infrastructure, and the Javascript is self-contained to the website. No impact is expected to any other systems.	Yes	NHIS	1	3	3		Approved 11th March 2020

specification#top											
The audit team does not have a current business continuity plan	3	3	9	The audit team to complete by 30th June 2020	Yes	Ceri Feltbower	2	3	6		30th June 2020

* SFHT Risk Assessment Matrix to be used

** if additional risks are identified please add to the notes section, Governance will add on completion of form.

Stage – 5 Legal Compliance

Compliance to be determined by NHIS/SFHT IG 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	• We only collect personal data we actually need for our specified purposes. • We have sufficient personal data to properly fulfil those purposes.

processed	
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.

Notes:

Click here to enter text.