Healthier Communities, Outstanding Care

Sherwood Forest Hospitals NHS Foundation Trust

# Data Protection Impact Assessment

| Title | Ref number |
|---|---|
| BadgerNet Maternity | |

## 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 | x | |
| Complete Project Details and check the Initial Screening Questions | x | x |

| | | |
|---|---|---|
| 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 | x | x |
| Initial Screening Questions to be formally written up and Introductory Meeting to be formally recorded | x | x |

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

**OR**

| If a Data Protection Impact Assessment **IS** required | | |
|---|---|---|
| **Activity** | **IAO/IAA** | **Governance** |
| When a new system is being implemented and the supplier provides a completed DPIA on a suppliers template, the information will need to be transferred to the Trust's template to ensure there are no omissions | **x** | |
| Complete Stage 2 – Data Protection Impact Assessment (Full) | **x** | |
| Complete Stage - 3 Identified Risks and Mitigating Action | **x** | |
| Complete Stage – 4 Legal Compliance | | x |
| Complete Assessment Summary & Recommendations for Action | x | |
| Account access management Standard Operating Procedure to be completed prior to the implementation of the project | x | |
| Closure meeting for final agreement | x | |
| Ensure Sign Off is completed | | x |
| Assessment shared with customer if appropriate | x | |
| Assessment to be kept with project documentation copy to Information Governance | x | |

**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:** | **BadgerNet Maternity** |

| **Project Description: Describe in sufficient detail for the proposal to be understood** |
|---|
| BadgerNet Maternity is a full end-to-end maternity electronic patient record system. Optional functionality includes real time CTG's (Cardiotocography), offline recording carried out away from the confines of the hospital. There is also a portal for birthing people to view and interact with their own notes; BadgerNotes. A Single Pregnancy Record is available, for Trusts, this allows to seamlessly share one record between multiple maternity services, ensuring continuity of care.<br>The data subjects are patients under the direct care of the Maternity Services at the Trust.<br>The current maternity information system sits in Orion Soprano Disease Management (SDM). Orion SDM is no longer supported and presents a significant cyber security risk to our Trust. A full procurement process has been undertaken and BadgerNet is the new system, supplied by Clevermed. |

| **Overview of the proposal: What the project aims to achieve** |
|---|
| • Utilise technology to improve patient safety and ultimately patient care and satisfaction.<br>• Reduce documentation burden and duplication.<br>• Reduce current data protection incidents.<br>• Improve reporting and audit capabilities; Locally and Nationally (MSDS)<br>• Ensure patients have access to their own maternity record, using BadgerNotes. |

| | |
|---|---|
| **Implementing Organisation:** | Sherwood Forest Hospitals NHS Foundation Trust |

| | |
|---|---|
| **Staff involved in DPIA assessment (Include Email Address):** | Claire Madon, Chief Nursing Information Officer<br>Alex Hague, Project and Business Change Manager<br>Lisa Butler, Deputy Head of Midwifery |

## Project Sign Off

| | Name | Job Title | Organisation | Date |
|---|---|---|---|---|
| **Information Asset Owner** | Lorraine Binch | Divisional General Manager | Sherwood Forest Hospitals NHS Foundation Trust | 29th November 2022 |
| **Data Protection Officer** | Jacquie Widdowson | Information Governance Manager | Sherwood Forest Hospitals NHS Foundation Trust | 16th November 2022 |
| **Information Governance** | Gina Robinson | Information Security Officer | Sherwood Forest Hospitals NHS Foundation Trust | 28th November 2022 |
| **Senior Information Risk Owner** | Shirley Higginbotham | Director of Corporate Affairs | Sherwood Forest Hospitals NHS Foundation Trust | 17th November 2022 |
| **Caldicott Guardian** | David Selwyn | Medical Director | Sherwood Forest Hospitals NHS Foundation Trust | 18th November 2022 |
| **Chief Digital Information Officer** | Richard Walker | Chief Digital Information Officer | Sherwood Forest Hospitals NHS Foundation Trust | 2nd December 2022 |

## 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**:<br><br>Legislative Compliance:<br><br>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.<br><br>Article 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)<br><br>Article 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<br><br>**Summary of Risks**:<br>Cyber security, loss of data, inappropriate access to data, inability to access data and Information Asset Management.<br><br>**Risks**<br><br>1. Loss of system access/data - Full system back-up process and business continuity plans in place<br>2. Data is accessed inappropriately due to lack of access controls. Movers and leavers access not removed. Data is inappropriately processed and/or disclosed<br>3. BadgerNet will need to be added to the divisional information asset register and the data flows mapped and recorded as part of the annual IAO returns to the SIRO |

## Recommendations for Action

| Summary of Identified Recommendations: | | |
|---|---|---|
| **Recommendations:**<br>Information Asset Administrators to ensure BadgerNet is added to the information asset register and data flows are mapped and recorded<br><br>Ensure business continuity plans are in place<br><br>Account management Standard Operating Procedure to be implemented, routine audit to take place | **Recommendation Owner:**<br>IAO | **Agreed Deadline for action:**<br>30th November 2022 |

## 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 | Full patient record will be collected including patient demographics and clinical information |
| **2** | Will the project compel individuals to provide information about themselves? | Y | Yes BadgerNet Maternity has areas of read and write for the patient to input on their own records through BadgerNotes |
| **3** | Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information? | Y | Patient Information will potentially be accessible to BadgerNet staff during deployment or any maintenance work. |
| **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 | Information will be used for the same purpose and not be utilised in a new format. The primary reason for data collection within the system is for clinical use |
| **5** | Are there processes in place to ensure data is relevant, accurate and up-to-date? | Y | Data is fed directly from CareFlow EPR using a HL7 feed which is covered by PAS data quality checks. |
| **6** | Are there security arrangements in place while the information is held? | Y | The national BadgerNet data is stored in the cloud with a local copy of the data on Trust managed servers. The BadgerNet HSCN server facility is hosted by an NHS approved and ISO27001 accredited supplier – Microsoft Azure |
| **7** | Does the project involve using new technology to the organisation? | N | Use of mobile technology within the Trust and is established. Community staff currently use laptops for recording patient care |
| **8** | Will the project result in you making decisions or taking action against individuals in ways which could have a significant impact on them? | Y | Information will be used in conjunction with direct patient care |

| Q | Screening question | Y/N | Justification for response |
|---|---|---|---|
| **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? | Y | 17.11.2022 A patient safety case has been undertaken in line with DCB0129 and DCB0160 |
| **10** | Is a Quality Impact/Technical Security Review required? | Y | 20.10.2022 - NHIS have reviewed the supplier assurance framework and have not identified any concerns or recommendations |

**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. | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| **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) | | | | | |
| | **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) | | Genetic or biomedical data | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| **2.2.2** | Is the data? | | | | | |
| | Identifiable? | ☒ | Pseudonymised? | ☒ | Anonymised? | ☐ |
| | If the data is pseudonymised please describe the technical controls in place ie pseudonymised data provided to a third party and the 'key' for re-identification to be retained by the Trust. Also describe how the data will be transferred ie using HL7 | | | | | |
| | The system contains a pseudonymised patient ID called the 'Badger ID'. This can be used in correspondence to refer to patients without recourse to standard identifiers such as NHS number or hospital number.<br><br>Protection at rest: Clevermed encrypts data where appropriate and feasible using 256-bit AES (Advanced Encryption Standard) encryption. This standard is used whenever encrypting data considered sensitive based on Clevermed's data classification protocols. Back up data is encrypted to the level of AES-256 bit. Wherever possible, for removable devices etc, Clevermed uses bitlocker to encrypt data at a device level.<br><br>Protection in transit: All desktop+iPad client-server communication is done over the HSCN network using HTTPS protocol over TLS1.2.<br><br>BadgerNet servers use standard Web Services, .Net Remoting, REST, and standard IIS page service for all communications with BadgerNet Client or Web Browser client. This is all done using HTTPS protocol over TLS1.2.<br><br>Within a hospital's local area network (LAN) communications to/from the local BadgerNet server (for FailOver Services) are done with standard port HTTP network links. Any communication between the local BadgerNet Server and the national HSCN BadgerNet servers is done over HTTPS using TLS 1.2 or greater. If a site required TLS1.2 traffic encryption within their local LAN whilst in failover mode, then they are responsible for installing a local domain-specific SSL certificate on that local server as needed.<br><br>Badger Notes: The data passing to and from the hospital records is encrypted using 256 bit-SSL encryption and sent via HTTPS over the internet. This includes data transferred in relation to the GP Access feature. | | | | | |

| | | |
|---|---|---|
| **2.3** | Is the data required to perform the specified task? | |
| | Y/N | Please justify response **Yes or No** |
| | Y | Full end to end Electronic Maternity Health Record for birthing person and child |
| **2.3.1** | How will you collect, use, store and delete data? | |
| | Data will be collected directly from the patient with a demographic and appointment feed from CareFlow EPR, Ultrasound Scan Reports will interface via | |

| | |
|---|---|
| | HL7 from CRIS. Nervecentre is being explored to extract the bed state into BadgerNet and a direct feed from BadgerNet into Nervecentre for observations<br><br>For web access we use TLS 1.2 or higher with strong cypher suites as defined by the National Institute of Standards and Technology (NIST) guidelines for Transport Layer Security (TLS) implementations. |
| **2.3.2** | What is the source of the data? (i.e. from data subject, system or other third party) |
| | Data subject, other clinical and non-clinical Trust systems |
| **2.3.3** | How much data will you be collecting and using? |
| | Full Maternity Record – Antenatal, Intrapartum, Postnatal |
| **2.3.4** | How often? (for example, monthly, weekly) |
| | Daily |
| **2.3.5** | How long will you keep it?<br><br>https://www.sfh-tr.nhs.uk/media/12002/isp-101-records-management-code-of-practice-2021.pdf |
| | In line with the current guidance of medical note retention<br><br>In respect of clinical records processed on behalf of the Trust, Clevermed provides reporting functions to allow identification of records approaching the retention threshold. It is the responsibility of the Trust to identify records reaching retention thresholds, review and issue written instruction on the action to be taken in respect of retention and destruction. No action will be taken in respect of record retention/destruction without the written instruction from the Trust. |
| **2.3.6** | Where will the data be stored? i.e., CareFlow, Shared Drive, offsite storage |
| | The national BadgerNet data is stored in the cloud with a local copy of the data on Trust managed servers. The BadgerNet HSCN server facility is hosted by an NHS approved and ISO27001 accredited supplier - Microsoft Azure. In the case of disaster recovery (e.g. data centre crashes) failover is activated to another Azure location in the UK. All BadgerNet data is held in the UK on UK servers and will not be transferred anywhere unless the Trust has instructed this. |
| **2.3.7** | How many individuals are affected? |
| | >30,000 |

| | | |
|---|---|---|
| **2.3.8** | What geographical area does it cover? | |
| | Local catchment area of Nottinghamshire, plus out of area patients who choose to receive maternity care at the Trust. | |

| | | |
|---|---|---|
| **2.4** | Who are the Organisations involved in processing (sharing) the data? | |
| | Organisations Name | Data Controller or Data Processor<br>*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.*<br>*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 |
| | Clevermed | Data Processor |
| | Microsoft | Sub Data Processor (hosting the data) |

| | | |
|---|---|---|
| **2.5** | If we have identified a supplier in 2.4, the following questions for 2.5 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** |
| | | As the Trust extracts and uploads the data to the online environment, there is no access to existing Trust network or systems. Microsoft is ISO27001 compliant https://docs.microsoft.com/en-us/compliance/regulatory/offering-iso-27001 |

| | | |
|---|---|---|
| | | Notts-HIS Supplier Assurance Framework |
| **2.5.1** | Please describe access and controls in place<br><br>Account access management Standard Operating Procedure to be completed prior to the implementation of the project<br><br>https://www.sfh-tr.nhs.uk/media/12007/ig-012-account-management-and-access-policy-2021.pdf<br><br>Account ManagementSOP Ten | |
| | Individual username and passwords to access BadgerNet<br><br>All Clevermed personnel are contractually obliged to adhere to the organisation's confidentiality and data security policies or face disciplinary action.<br><br>BadgerNotes users are specifically counselled via privacy notice on maintenance of password security.<br><br>Badgernet - Account Management and Acc | |
| **2.5.2** | Please provide a copy of the contract in place | |
| | Scan-2022-10-05-10-35-32-810-11197.pdf<br>Appendix A - Call-off Terms and Conditions<br><br>Joint procurement with Nottingham University Hospitals NHS Trust. | |
| **2.5.3** | Have arrangements for retention and destruction been included in the contract when the service/contract expires?<br><br>https://www.sfh-tr.nhs.uk/media/12002/isp-101-records-management-code-of-practice-2021.pdf | |
| | Clevermed adheres to the data retention guidance specified by the document 'The Records Management Code of Practice 2021' and relevant legislation pertaining to the retention of specific non-clinical record types. In respect of clinical records processed on behalf of the | |

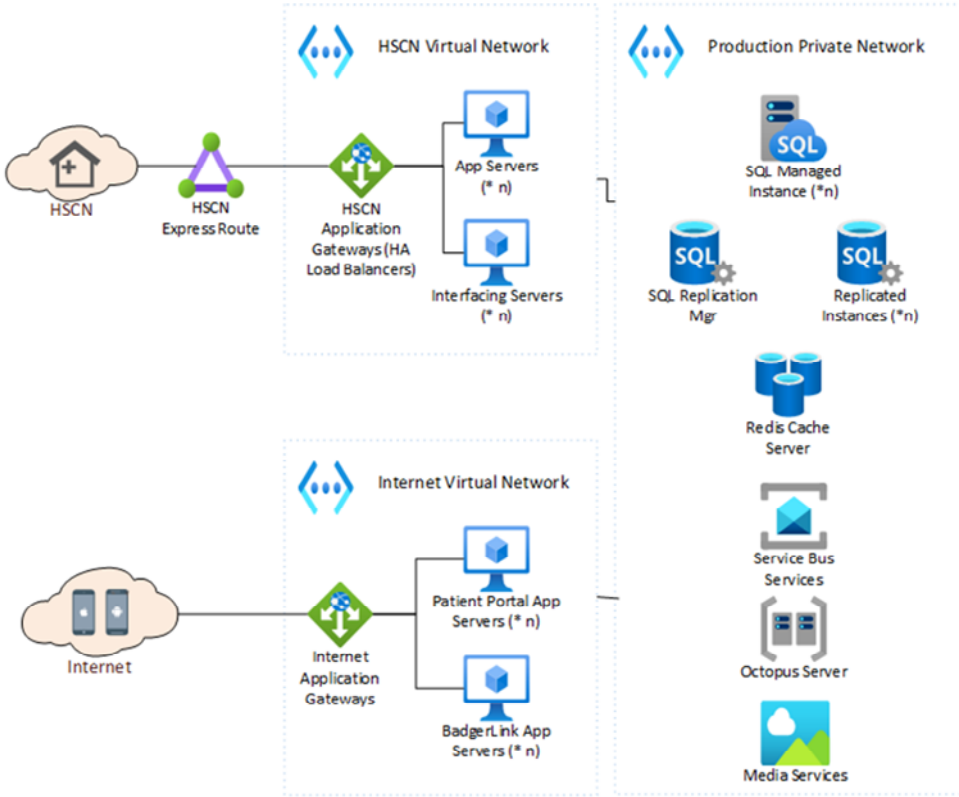
| | | | |
|---|---|---|---|
| | Trust, Clevermed provides reporting functions to allow identification of records approaching the retention threshold. It is the responsibility of the Trust to identify records reaching retention thresholds, review and issue written instruction on the action to be taken in respect of retention and or destruction. No action will be taken in respect of record retention/destruction without the written instruction of the Trust.<br><br>BadgerNotes: Users will continue have access to the app and the user information necessary for portal access will be retained for processing until such time as:<br>-The app is rendered obsolete<br>-The records reach the end of their retention period<br>-The user cancels their access via the app | | |
| **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 Enforcement? Please check the register | Yes | No |
| | | | **x** |
| **2.5.6** | Has the supplier received ICO Decision Notice? Please check the register | Yes | No |
| | | | x |
| **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 | 31st March 2022 | 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 | Cyber Essentials certificate 061222.pdf<br>CE only | |
| | ISO 15489 Records Management | | x |
| | ISO 27001 Information Security Standards | ISO27001Certno161211exp191125.pdf | |
| | ISO 9001 Quality Management Systems | ISO9001Certno042115exp191125.pdf | |

| | | |
|---|---|---|
| **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 | |
| | Not applicable | |
| **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 | BadgerNet is a shared care record system. Each clinical record of care for an individual patient at a distinct care location is held on the Platform. Only authorised users of the Platform with appropriate rights and privileges can enter data for a patient with an episode of care at their care location. The clinical record for an individual patient will be authorised to be shared with a subsequent care location using the Platform by the act of the clinicians discharging or transferring the patient within the Platform. In order for the record of care to be viewed in a subsequent care location(s), the subsequent care location(s) must then admit or transfer the patient in to |

| | | |
|---|---|---|
| | | their care location on the Platform. In all cases, the record can only be viewed by users of the Platform who have been given the appropriate rights and permissions. Access rights are assigned by a member of the Trust whose role and responsibility is designated as BadgerNet User Manager. |
| **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 | Clevermed would only require access to Trust servers via a formal request in order to provide support/management of the BadgerNet system on the Trust servers |
| **2.8** | Has a data flow mapping exercise been undertaken? | |
| | Y/N | If **Yes**, please provide a copy here. If No, please explain why |
| | 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 explain why | |




Data flows will need to be mapped once the service has gone live, added as a risk

| | | | | | | |
|---|---|---|---|---|---|---|
| **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 | Both the Trust and Clevermed can audit the system, it's built in such a way that "audit" is available in most screens i.e. it shows who last updated it and at what time. More in depth audits can be undertaken but "senior users" with the correct user permission. |

| | | |
|---|---|---|
| **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** |

| | | |
|---|---|---|
| | Y | This data will be used in accordance with CareFlow EPR for the demographics and other Trust systems such as Nervecentre, CRIS, and Rhapsody etc, this will be transformational for department as they are moving to a paperlite documentation schema, with ambitions to become paper free. Some information will be transmitted to other providers such as Health Visitors and GP's via current Trust processes in line with data sharing agreements. Clevermed have on their roadmap for next year FIHR messaging which would remove PDF's and introduce structured fields, in line with national "ambitions". Medicine TTO's will continue to be undertaken in Orion until maternity are scheduled to take ePMA |

| | |
|---|---|
| **2.12** | How will the information be kept up to date and checked for accuracy and completeness? (data quality)<br>How will you ensure data minimisation? |
| | Data will be accessed by a number of clinicians with appropriate access based on role based access controls and a 'lighter' version of the record will be also available to the patient. |
| **2.13** | Who will have access to the information? (list individuals or staff groups) |
| | Midwives<br>Health Visitors<br>Obstetricians<br>Sonographers<br>Therapists<br>Registered Nurses working within maternity<br>Paediatricians<br>Anaesthetists<br>Administrators<br>Data subjects (patients)<br>PKB is likely to be on the roadmap in the future to align with the ecosystem |

| | | |
|---|---|---|
| | Proxy access can be granted by the birthing person to another clinician such as a GP to review the record for a time limited period. i.e. max. 1hr. | |
| **2.14.1** | 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 ( baton devices) | ☒ |
| | 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) | ☐ |
| | Any NHIS users will need to use a Username and Password as Active Directory will only work for Trust users due to the domain. Eventually when all users are on NHIS domain we can ensure all users use Active Directory.<br><br>With regards to the device security, this is in line with Trust policy for devices. They are protected with Airwatch encryption, the level of passcode to secure the device is dictated by policy (6 digits for the Apple devices) as is how the devices are handled and how long until they automatically lock etc.<br><br>With regards to the Application; staff have unique log on from their Trust Active Directory log ins. They are assigned a role which dictates what information they can see/ have access to. Locums who require access and do not have a current Active Directory account are able to sign up to a temporary account with their details. This is authorised within the application by a senior member of staff. All audit data for this will then be stored in the application. | |

| | | | | |
|---|---|---|---|---|
| **2.14.2** | What physical security measures have been implemented to secure access? ie swipe cards, digilock | | | |
| | Information is stored electronically. Physical access to the server rooms and remote access to the servers is restricted to those who require access to perform their duties. CCTV is in operation | | | |
| **2.15** | Will the data be stored on Trust servers | | | |
| | Yes | No | | |
| | Yes and a copy is held in Microsoft Azure data centre | | | |
| **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 | ☐ |
| | Other | ☒ | please specify below | ☐ |
| | Protection at rest: Clevermed encrypts data where appropriate and feasible using 256-bit AES (Advanced Encryption Standard) encryption. This standard is used whenever encrypting data considered sensitive based on Clevermed's data classification protocols. Back up data is encrypted to the level of AES-256 bit. Wherever possible, for removable devices etc, Clevermed uses bitlocker to encrypt data at a device level.<br><br>Protection in transit: All desktop+iPad client-server communication is done over the HSCN network using HTTPS protocol over TLS1.2. BadgerNet servers use standard Web Services, .Net Remoting, REST, and standard IIS page service for all communications with | | | |

| | | |
|---|---|---|
| | BadgerNet Client or Web Browser client. This is all done using HTTPS protocol over TLS1.2.<br>Within a hospital's LAN communications to/from the local BadgerNet server (for FailOver Services) are done with standard port HTTP network links. Any communication between the local BadgerNet Server and the national HSCN BadgerNet servers is done over HTTPS using TLS 1.2 or greater. If a site required TLS1.2 traffic encryption within their local LAN whilst in failover mode, then they are responsible for installing a local domain-specific SSL certificate on that local server as needed.<br><br>Badger Notes: The data passing to and from the hospital records is encrypted using 256 bit-SSL encryption and sent via HTTPS over the internet. This includes data transferred in relation to the GP Access feature. | |
| **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 | All core BadgerNet data is stored in one of the Azure SQL Managed Instances in Azure UK South. One of the key features of this PaaS service are their extensive business continuity features. As part of the service offering, all SQL Managed Instances automatically create full database backups weekly, differential database backups every 12 hours, and transaction log backups every 5 -10 minutes. The backups are replicated to a secondary Azure geographic location (RA-GRS)storage for at least 7 days. All SQL instances provide7-daypoint-in-time restore. |
| **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 | Staff undertake annual data security awareness level 1 training |
| **2.19** | Will reports be produced? | |

| | | |
|---|---|---|
| | Will reports contain personal/sensitive personal or business confidential information? | At times it may be relevant to share sensitive information internally |
| | Who will be able to run reports? | Information team, NHIS, Digital Nursing Team, System Users with the "reporting" access right. |
| | Who will receive the reports and will they be published? | Trust staff who request / require information for audit purpose |

| | | |
|---|---|---|
| **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 | In the event of contract termination and/or a permanent data deletion request, the Trust will need to provide a written request signed by an approved representative, at which point Clevermed will export all data held on behalf of the Trust in a secure encrypted format. This export will include all the raw XML care record data, raw binary trend monitoring and CTG data (where applicable), plus any standardised reporting database extract databases. This will be provided in a standard SQLServer extract file which can be imported into any SQL server at the Trust's discretion. There are no charges for the return of the data via the method specified above. If any bespoke data transformation is required a quote will be provided following functional specification of the requirements. Once the data has been exported, it will then be securely and permanently deleted from the Platform according to the procedures outlined within the Secure Disposal of |

| | | |
|---|---|---|
| | | Media appendix of the data security and use policy (embedded below). In the event that the record to be deleted forms part of a shared care record, the record will remain within the BadgerNet Platform unless the deletion has been approved by all joint Data Controllers<br>  <br>Clefvermed Data Security and Use Pol |
| **2.21** | Is consent required for processing of personal data? | |
| | Y/N | Please describe if answered **Yes** |
| | N | Direct care |
| | | 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? |
| | N | Part of our statutory duties under UK GDPR 6(1)(e) public interest or public duty, and UK GDPR 9(2)(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services. |
| **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 | The Trust's privacy notice is here https://www.sfh-tr.nhs.uk/for-patients-visitors/your-medical-record/ |
| **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 | Removal of a patients record would require the supplier to do so. Any information recorded in error can be struck |

| | | |
|---|---|---|
| | | through by the user and is based on role based access controls |
| **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 | Direct care to the patient and recording clinical information to support their care |
| **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 policy and procedure for responding to subject access requests. Further information for patients on how to access their records is here: Sherwood Forest Hospitals (sfh-tr.nhs.uk).<br><br>Access to Health Records staff will be given access and trained how to extract data. |
| **2.26** | Who are the Information Asset Owner(s) and Administrator(s)? | |
| | IAO | Divisional General Manager, Women and Children's |
| | IAA | Melanie Butcher, Digital Midwife<br><br>Paula Shore, Clinical Risk Midwife |
| | System Administrators | Application Support, NHIS & Digital Midwife |
| **2.27** | How is the data secured in transit and at rest? Eg encryption, port control number | |
| | Protection at rest: Clevermed encrypts data where appropriate and feasible using 256-bit AES (Advanced Encryption Standard) encryption. This standard is used whenever encrypting data considered sensitive based on Clevermed's data classification protocols. Back up data is encrypted to the level of AES-256 bit. Wherever possible, for removable devices etc, Clevermed uses bitlocker to encrypt data at a device level. | |

| | | |
|---|---|---|
| | Protection in transit: All desktop+iPad client-server communication is done over the HSCN network using HTTPS protocol over TLS1.2.<br>BadgerNet servers use standard Web Services, .Net Remoting, REST, and standard IIS page service for all communications with BadgerNet Client or Web Browser client. This is all done using HTTPS protocol over TLS1.2.<br>Within a hospital's LAN communications to/from the local BadgerNet server (for FailOver Services) are done with standard port HTTP network links. Any communication between the local BadgerNet Server and the national HSCN BadgerNet servers is done over HTTPS on port 443 using TLS 1.2 or greater. If a site required TLS1.2 traffic encryption within their local LAN whilst in failover mode, then they are responsible for installing a local domain-specific SSL certificate on that local server as needed.<br><br>Badger Notes: The data passing to and from the hospital records is encrypted using 256 bit-SSL encryption and sent via HTTPS over the internet. This includes data transferred in relation to the GP Access feature. | |
| **2.28** | 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.**<br>Please state what checks were undertaken if response is answered **No.** |
| | Y | A patient safety case and supplier assurance framework have been reviewed and signed off. |
| **2.29** | Are there any current issues of public concern that you should factor in? | |
| | Y/N | Please describe if answered **Yes.** |
| | N | |
| **2.30** | 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? | |
| | Provide an end to end paperlite maternity record with both read and write facility to the birthing person<br><br>Increase patient safety both for birthing person and child | |

| | |
|---|---|
| | Reduce paper processes and documentation burdens<br><br>Increase ease of obtaining data and audit to shape improvements in patient care<br><br>Provide single MIS-R across Nottingham and Nottinghamshire |
| **2.31** | Consider how to consult with relevant stakeholders:<br><br>• Describe when and how you will seek individuals' views – or justify why it's not appropriate to do so.<br>• Who else do you need to involve within your organisation?<br>• Do you need to ask your processors to assist? |
| | Alex Hague, Project and Business Change Manager presented this document to the Information Governance working group for consultation. |

| | |
|---|---|
| **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**<br><br>**Legal basis: patients**<br><br>**Personal data i.e. name, address**<br><br>6(1)(a) the patient has given consent<br><br>6(1)(c) necessary for legal obligations<br><br>6(1)(e) public interest or public duty<br><br>6(3) the above supported by Member State law (UK legislation as applicable to circumstances)<br><br>**Sensitive personal data (special category)**<br><br>9(2)(a) the patient has given explicit consent<br><br>9(2)(c) processing for 'vital interests' (safety, safeguarding, public safety, etc.)<br><br>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.<br><br>9(2)(j) (together with Article 89 and relevant recitals) relates to archiving, statistical analysis and research.<br><br>**Legal basis: staff** – please review Appendix 10 Information Sharing Protocol for further information). |
| | The Trust's lawful basis for processing personal and special categories of personal data are:<br><br>1. UK GDPR 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.<br><br>2. UK GDPR Article 9(2)(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject<br><br>3. UK GDPR Article 9(2)(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services.<br><br>Supplier<br><br>1. UK GDPR 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.<br><br>2. UK GDPR Article 9(2)(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services. |
| **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) |

| | |
|---|---|
| | This DPIA will be published once finalised. The Trust's privacy notice has been updated. Patients are informed during a consultation with clinicians that information is being recorded electronically |

| | |
|---|---|
| **2.34** | What measures do you take to ensure processors comply? |
| | The Trust is aware that Clevermed contract Microsoft to provide their data hosting environment. The Trust and Clevermed have a contract in place and this will be reviewed on a regular basis. |
| **2.35** | How will you prevent function creep? Manage lifecycle of system/process |
| | Clevermed will only ever process the Trust's data as per explicit agreement with the Trust<br><br>The Trust and Clevermed have a contract in place where roles and responsibilities are defined.<br><br>To prevent function creep, processing activity will be carried out on behalf of the Trust by Clevermed that is agreed to. The Service Agreement provides explicit information on processing activity provided by Clevermed as part of offering the BadgerNet System. There is limited scope to utilise the platform for other functions within the Trust. As data controller, the Trust has full responsibility for ensuring health care professionals accessing the system utilise it appropriately. |

# Stage - 3 Risk Template

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

| Completed by: Claire Madon | Role: CNIO | Date completed: 2nd March 2022 |
|---|---|---|

| **Risk description**<br>What event could happen which would impact on the activity?<br>What would cause it to happen?<br>What would the consequence be? | **Primary controls**<br>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**<br>If the risk is not controlled to an acceptable level, what are the issues that need to be addressed? | **Acceptable risk** | | | **Mitigating actions required**<br>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)** | |
| Loss of system access due to connection failure or server failure either via NHIS or 3rd party supplier.<br><br>This could result in the service being disrupted or unavailable.<br><br>The consequences of this could be patient harm, financial penalties and reputational damage to the Trust | Full system back-up processes and ISO 27001 accreditation in place<br><br>Business Continuity plan for the BadgerNet system is in place | 2 | 2 | 4 | | 2 | 2 | 4 | Manual input, business continuity plan to be used. Business continuity plan reviewed annually |

| **Risk description**<br>What event could happen which would impact on the activity?<br>What would cause it to happen?<br>What would the consequence be? | **Primary controls**<br>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**<br>If the risk is not controlled to an acceptable level, what are the issues that need to be addressed? | **Acceptable risk** | | | **Mitigating actions required**<br>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)** | |
| Loss of system data due to connection failure or server failure either via NHIS or 3rd party supplier.<br><br>This could result in the service being disrupted or unavailable.<br><br>The consequences of this could be patient harm, financial penalties and reputational damage to the Trust | Full system back-up processes and ISO 27001 accreditation in place<br><br>Business Continuity plan for the BadgerNet system is in place | 2 | 2 | 4 | | 2 | 2 | 4 | Manual input, business continuity plan to be used. Business continuity plan reviewed annually |
| 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. Any NHIS users will need to use a Username and Password as AD will only work for SFH users due to the domain. Eventually when all users are on NHIS domain we can ensure all users use AD. Account Management and access procedure to be completed. Appropriate access according to role. | 2 | 2 | 4 | | 2 | 1 | **2** | Ensure access is managed and leavers list is received and actioned. Routine audits. Information governance training up to date |

| **Risk description**<br>What event could happen which would impact on the activity?<br>What would cause it to happen?<br>What would the consequence be? | **Primary controls**<br>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**<br>If the risk is not controlled to an acceptable level, what are the issues that need to be addressed? | **Acceptable risk** | | | **Mitigating actions required**<br>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)** | |
| | Data Processor: Clevermed staff – ISO9001, access protocol for decommissioning of systems access at termination. Use of two factor authentication for Maternity Notes application features, including GP access.<br><br>IG training in place<br><br>BadgerNet contains full audit trail and access logs so that unauthorised or unsanctioned uses can be tracked.<br><br>BadgerNet contains a data access warning.<br><br>BadgerNet allows records to be set as ‘sensitive’ to require explicit reason for access to be documented before a record can be accessed.<br><br>Where the national single pregnancy record is in use, a patient can only be searched for in the system via NHS number to deter casual querying. | | | | | | | | Ensure adequate access controls are in place. |

| **Risk description**<br>What event could happen which would impact on the activity?<br>What would cause it to happen?<br>What would the consequence be? | **Primary controls**<br>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**<br>If the risk is not controlled to an acceptable level, what are the issues that need to be addressed? | **Acceptable risk** | | | **Mitigating actions required**<br>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)** | |
| | Where the national single pregnancy record is in use all access to records at another organisation not delivering care is via break glass which requires the user to specify the reason for access.<br><br>Where the national single pregnancy record is in use, each organisation can see a fully audited report on which records at their unit have been accessed via Break Glass and by whom. They can also access a report detailing which records have been accessed via break glass by members of the organisation. All break glass events are documented in the medical record. | | | | | | | | |
| If the system is not recorded on the information asset register, the system may not be brought back online in response to a cyber attack | In the Trust we have a business continuity plan if the service was unavailable. The department would default back to the current practice and access the information manually | 2 | 2 | 4 | BadgerNet will need to be added to the divisional information asset register and the data flows mapped and recorded as part of | 2 | 1 | **2** | BadgerNet will need to be added to the divisional information asset register and the data flows mapped and recorded as part |

| **Risk description**<br>What event could happen which would impact on the activity?<br>What would cause it to happen?<br>What would the consequence be? | **Primary controls**<br>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**<br>If the risk is not controlled to an acceptable level, what are the issues that need to be addressed? | **Acceptable risk** | | | **Mitigating actions required**<br>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)** | |
| | | | | | the annual IAO returns to the SIRO | | | | of the annual IAO returns to the SIRO |

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 –**<br>Personal data shall be processed fairly and lawfully and, in a transparent manner | Lawfulness<br>• We have identified an appropriate lawful basis (or bases) for our processing.<br>• We are processing special category data and have identified a condition for processing this type of data.<br>• We don't do anything generally unlawful with personal data.<br><br>Fairness<br>• We have considered how the processing may affect the individuals concerned and can justify any adverse impact.<br>• We only handle people's data in ways they would reasonably expect, or we can explain why any unexpected processing is justified.<br>• We do not deceive or mislead people when we collect their personal data.<br><br>Transparency<br>• We are open and honest, and comply with the transparency obligations of the right to be informed. |
| **Principle 2 –**<br>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.<br>• We have documented those purposes.<br>• We include details of our purposes in our privacy information for individuals.<br>• We regularly review our processing and, where necessary, update our documentation and our privacy information for individuals.<br>• 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 –**<br>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.<br>• We have sufficient personal data to properly fulfil those purposes. |
| **Principle 4 –**<br>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.<br>• We have appropriate processes in place to check the accuracy of the data we collect, and we record the source of that data.<br>• 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.<br>• If we need to keep a record of a mistake, we clearly identify it as a mistake.<br>• Our records clearly identify any matters of opinion, and where appropriate whose opinion it is and any relevant changes to the underlying facts.<br>• We comply with the individual's right to rectification and carefully consider any challenges to the accuracy of the personal data.<br>• As a matter of good practice, we keep a note of any challenges to the accuracy of the personal data |
| **Principle 5 –**<br>Kept no longer than is necessary | • We know what personal data we hold and why we need it.<br>• We carefully consider and can justify how long we keep personal data.<br>• 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 –**<br>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.<br>• We use encryption.<br>• We understand the requirements of confidentiality, integrity and availability for the personal data we process.<br>• 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.<br>• 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.<br>• We implement measures that adhere to an approved code of conduct or certification mechanism.<br>• We ensure that any data processor we use also implements appropriate technical and organisational measures. |