GROW 2.0
Data Privacy Impact Assessment

Version 1.2

Distribution

This document is available for public viewing on the DTAC page of our company website
perinatal.org.uk/information/dtac

Document Status

This document is version controlled. Whilst it may be printed, the electronic version is the controlled copy. Any printed copies of this document are not controlled.

Table of Contents

1 | Introduction

This Data Privacy Impact Assessment (DPIA) applies to GROW 2.0 provided by the Perinatal Institute as part of the GAP Programme. GROW 2.0 is available both as a web application and as API for trusts/hospitals. From the screening process, information/data processing with high risk to individuals was identified, that *might be* likely to occur. A DPIA was deemed mandatory for this project to explore this risk likelihood further. The risk assessment concluded there were no high-level risks left uncontrolled or insufficiently controlled. The high risk identified to an individual was unlikely to occur. All risks have been effectively controlled.

Collectively 'GROW 2.0 App' and 'GROW 2.0 API' will be referred to as 'GROW 2.0' here on.

This checklist is to be used by the Information Governance Team when assessing compliance with the UK General Data Protection Regulation involved in the processing of person identifiable data (PID).

All processing of PID must be tested for data protection/confidentiality compliance prior to implementation/commencement and approved by the Information Governance Steering Group. This process is in line with the Information Commissioner's Office DPIA Code of Practice. In accordance with the UK General Data Protection Regulations (UK GDPR) Article 35, DPIAs are mandatory for the processing of high-risk information processes.

The Perinatal Institute is a processor on behalf of the trust/hospital as the controller with GROW 2.0. If the GROW 2.0 API is integrated via an additional party, (e.g., through an MIS system) then the Perinatal Institute is a processor on behalf of both the trust/hospitals and MIS's/parties.

Please note – GROW 2.0 is a newer upgraded and separate system, to the previous GROW systems running on versions 1.0 to 1.5. There is a separate DPIA for the pre 2.0 versions of GROW, as it is a pseudonymised system. GROW 2.0 is a patient/personal identifiable system to which this DPIA is targeted.

GROW 2.0 is a registered Medical Device through MHRA.
GROW 2.0 information can be found here: perinatal.org.uk/grow2.0/
GROW 2.0 implementation documentation can be found here:
perinatal.org.uk/grow2.0/documentation

2 | Background

The Perinatal Institute is a not-for-profit organisation that licences GROW software as part of its GAP programme. GROW customised growth charts are produced since 2001 and are now used in up to 80% of pregnancies in the UK.

Implementation of the GAP programme within England has resulted in increases in the antenatal detection of SGA babies accompanied by significant, year on year reductions in stillbirth. Using customised growth charts based on maternal characteristics is now seen as standard practice in the assessment of fetal growth and wellbeing and hospitals use auto reporting within the GROW application to audit care and action improvements in practice. The pseudonymised GROW data also enabled improvements in the coefficients within GROW, so the charts are more precise at identifying abnormal growth and babies at risk in utero.

Due to the ongoing drive for digital health and national initiatives such as Better Birth (2016) to go 'paperless/paper-light', the PI set out to accomplish these best practice recommendations by developing a new version of GROW which:

- Provides a fully electronic customised chart with auto plotting of fetal growth measurements during pregnancy, decision-making support that alerts clinicians of risks

and abnormal growth, and calculation of the birthweight centile to assist in postnatal management.
- Provides all caregivers across the UK and the mother access to the GROW record

3 | The need for a DPIA

UK GDPR requires data controllers/processors to complete a DPIA before any type of data processing which is 'likely to result in a high risk to the rights and freedoms of natural persons'.

GROW 2.0 collects, processes, transmits and stores personal data (including patient data). Some personal data items are manipulated for encryption. For research purposes, data is fully anonymised.
GROW 2.0 processes personal data to enable the production of customised growth charts and birthweight centiles to assess fetal growth during pregnancy and birth. Personal data is stored within the GROW 2.0 database where individuals can be identified.

Due to the above, to comply with UK GDPR, transparency and clear responsibilities between controllers and processors need to be implemented for GROW 2.0, which this DPIA supports.

This DPIA will enable the Perinatal Institute to identify and minimise the risks relating to personal data processing activities while informing relevant parties or audiences. From screening questions, this DPIA was carried out to assess the likelihood versus the severity of risk for 'high risk' processing.

4 | Data processing

The Perinatal Institute processes personal information on behalf of the controller. Section 4 summarises these data processing activities under UK GDPR and Data Protection Act 2018.

For GROW 2.0:
The Perinatal Institute is a processor only – on behalf of the controller or sometimes controllers. The trust/hospital is a controller, usually the sole primary controller.

If a trust/hospital chooses to integrate with GROW 2.0 and use a third party such as an MIS (e.g. to integrate GROW 2.0 API) – the third party/MIS may also be a controller with the trust/hospital, either with primary and/or secondary responsibilities or as a joint controller. In this scenario, the Perinatal Institute may process on behalf of two or more controllers.

Either a data processing agreement, multi-party data processing agreement, data sharing agreement and/or data pool agreement should always be considered.

It is important to highlight, in addition to the clinical use of GROW 2.0 by trusts/hospitals, there is also 'GROW 2.0 Mother's App' that allows mothers to login and view their personal data as read-only. The trust/hospital is the controller for this data to provide direct care.

4.1 | Scope/Subject matter of the processing

Personal data is processed and stored within GROW 2.0 (2.0 web application and/or 2.0 API), on all mothers during pregnancy and birth that have their care provided by hospitals in the GAP programme. GROW 2.0 uses this stored data to display this information back in a useful way clinically, inside the application itself.

The controller's (trust/hospital) primary processing justification typically references:

- Implied consent as the lawful basis (under common law)
- Affirmative action, e.g., through Article 9(h) (UK GDPR)

- NHS England provides additional legal basis for processing data here: england.nhs.uk/contact-us/privacy-notice/nhs-england-as-a-data-controller/
 - which individual trusts/hospitals may also reference.
(Different Trusts/hospitals as controllers may differ on what Articles they choose to control/process personal data under).

This is because GROW assists clinicians in providing direct care throughout pregnancy, birth, and the postnatal period. The Perinatal Institute is a processor on behalf of the controller for this subject matter.

Personal data is stored for the standard medico-legal requirement of 25 years and an audit trail of all actions are logged. Where the GROW 2.0 record is produced via the 2.0 GROW-API, the maternity information system also logs all activity in their audit trail.

4.2 | Nature of the Processing / Data Processing Scenarios

The following six operations exist within GROW 2.0 with the nature of processing for personal data.

1. **GROW 2.0 App – Personal data is:**
    - Received/retrieved (data entered by trust/hospital only)
    - Unique chart identifier created
    - Personal data stored in GROW 2.0 database
    - Specific data types are manipulated for encryption (security)
    - All relevant personal data displayed back inside the application
    - Optional to be transmitted to a paper-based printable chart (.PDF)

The printable option is processed to provide the trust/hospital with a paper-based copy if they choose to.

2. **GROW 2.0 API – Personal data is:**
    - Received/retrieved (data entered by trust/hospital, sometimes passed through via MIS or third-party integration chosen by trust/hospital.)
    - Unique chart identifier created
    - API calls - typically creation or modification of personal data request is sent, processed, and stored in GROW 2.0 database. Personal data response is sent back through the API back to the sender in JSON format. The API works on a request and response basis.
    - Specific data types are manipulated for encryption (security)
    - All relevant personal data sent through API can be displayed back inside the application

3. **Research purposes – data anonymisation:**
    The Perinatal Institute uses data collected in the application from pregnancy episodes and fully anonymises it for research purposes, according to the Information Commissioner's Code of Practice: ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf

4. **Read-only mother access:**
    Mothers have read-only access to their personal data, for which the controller is responsible.
    The controller may request the Perinatal Institute to make changes as a processor on their behalf
    e.g. 'Rights to Individuals' – see point 5.

5. **Helpdesk processing requests on behalf of the controller:**
    Controllers can make helpdesk requests to the Perinatal Institute for processing requests on their behalf.
    This may include operations such as:

- Data change requests
- Audit report requests

These types of requests may also include ‘Rights to Individuals’ under UK GDPR, e.g., right to rectification. Although controllers are responsible for ‘Rights to Individuals’ the Perinatal Institute can assist when requested, and process on behalf of the controller for the scenarios listed below:

The trust/hospital can request a data change via the Perinatal Institute helpdesk (outlined in Service Level Agreement). This is where the Perinatal Institute could modify data in GROW 2.0 as a processor, on behalf of the trust/hospital as a controller. Data being modified will be used by the trust/hospital to provide direct care in most circumstances. As a clinical safety precaution, the trust/hospital cannot delete a mother or delete data/information, it can only be edited. This is the main purpose of a data change request in GROW 2.0 is to make a deletion request.

Types of data change requests:

- Delete data from mother record:
  The trust/hospital has added information to the wrong mother and requires deletion. The trust/hospital can edit this information but would require the Perinatal Institute to delete this information in the first release. Subsequent releases will allow HCLA’s to delete information, but the audit trail will remain.

- Change to data that may alter reports:
  The trust/hospital has added incorrect information of any kind e.g., measurement, duplicated mother record, risk review, care plan etc. The trust/hospital can edit this information but would require the Perinatal Institute to delete this information in the first release. A change to this data may affect reports.
- Merge record:
  A trust/hospital may require records to be merged, e.g., if two different hospitals have the same mother but a different spelling on the same person’s name, which could cause separate records to be created. A merge request can be made in this case.

The Perinatal Institute would be the processor on behalf of the trust/hospital as a controller for all the above types of data change requests.

Audit report request
The trust/hospital can request a mother record audit report via the Perinatal Institute helpdesk (outlined in Service Level Agreement). This is where the Perinatal Institute could provide a ‘data dump’ of the mother record as a CSV file. The Perinatal Institute would be the processor on behalf of the trust/hospital as a controller.

6. **Amazon Web Services (AWS) act as a data processor**
   Under UK GDPR, Amazon Web Services (AWS) can act as both a data controller and data processor. However, for GROW 2.0 they act as a data processor (passively) only and not a controller. AWS provide the hosting infrastructure where it is the responsibility of the Perinatal Institute to put security measures in place to protect the GROW 2.0 hosted service and data/information stored within. AWS provide full documentation that is publicly available on these conditions:

- AWS GDPR compliance statement: aws.amazon.com/compliance/gdpr-center/
- AWS GDPR data processing addendum: d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf
- AWS Terms of Service: aws.amazon.com/service-terms/

4.3 | Context of Processing

The Perinatal Institute process data on behalf of the controller so they can provide care. It can access personal data for processing purposes on behalf of the controller. The Perinatal Institute's relationship for GROW 2.0 exists between the trust/hospital and sometimes MIS/integration provider with GROW 2.0 API. The public is free to call the office number, but any type of patient care or patient information will not be provided.

The Perinatal Institute uses anonymised data for research purposes (explained further in Section 4.9 & 4.12), to assist controllers and the health service in general to provide improved levels of care. The Perinatal Institute provides training as part of the GAP Programme for best practice when using GROW 2.0, however, it is ultimately at the controller's discretion how they use their data.

The Perinatal Institute does not sell, rent, or trade personal data to any third parties. All access to personal data is solely for the purposes of delivering agreed processing services on behalf of the controller. The Perinatal Institute strictly adheres to UK GDPR and ethical guidelines, and does not use personal data for any purpose beyond those contractually and legally defined.

4.4 | Purposes for Processing

The purpose of GROW 2.0 as part of the GAP programme is to provide improved levels of maternity care, where the Perinatal Institute provides GROW 2.0 as a tool for controllers to utilise, to enhance direct care to mothers and babies. By processing data, the Perinatal Institute strives to continue reducing stillbirth rates year on year, both in the UK and globally by facilitating access and training for proper usage of these tools. To achieve this, personal information must be processed on behalf of the controller. All personal data items stored/processed are required for providing the advanced support features GROW 2.0 provides over the previous GROW (versions below 2.0) e.g., auto plotting and automated risk factor alerts.

Further GAP information can be found below:
perinatal.org.uk/GAP/Programme
perinatal.org.uk/GAP/Uptake
perinatal.org.uk/FAQ

4.5 | Types of Personal Data – Data Types/Datasets

The most common list of personal data types/data items processed are listed below.
For the full list, see the bottom of this document in section '10 | Appendix 1 - Data Items (Full list)'.

Common Data Items:

Maternal		
Forename	Surname	NHS No.
DOB	Postcode	Email address
Phone number	Ethnicity	Hospital number
EDD	Weight @ booking	Height
Risk factors for SGA	Plan of care details	Next appts
SFH / EFW/ Doppler measurements	Last menstrual period	Previous babies
Parity		

Baby		
NHS Number	DOB & time of birth	Gestation
Sex	Birthweight	Referral/ detection SGA/FGR
Unit responsible for AN care	Birth complications	BW centile
Resuscitation	Mode of birth	Apgar score
Destination of transfer	Neonatal Plan of care	

Previous Pregnancies		
Number of previous babies	DOB	Gestation
Outcome	Birthweight	Centile
Sex	Name	

List of Datasets:

Mother demographics
Stored to ensure correct mother record is held and accessed to maintain integrity and confidentiality of patient's records.

Current pregnancy
Details of current pregnancy needed to provide direct care and manage risks following assessment.

Estimated Date of Delivery
Data is required to create a customised chart and add measurements of both fundal height and estimated fetal weights, from USS examinations to the correct gestation.

Previous pregnancies
Required to assess if previous pregnancy outcomes may affect care or risk status.

Risk assessment
To document risk status/actions from assessment as per care.

Add fundal height measurements.
For routine care and assessment

Add scan measurements EFW and Doppler.
For care and assessment

Centile
Created and recorded for pregnancy outcome and plan of care for neonate.

4.6 | Categories of Data Subject

- Mother
- Baby

4.7 | Duration of Processing

As supported by a data processing agreement and/or data sharing agreement: *'This Agreement shall commence on the date of its signature by the Parties and remain in effect for a term of one year. Upon expiry, the Agreement shall automatically renew for a further period of one year, and thereafter on each anniversary of the Agreement commencing, unless terminated or renegotiated by either Party*

Either Party may terminate or re-negotiate this Agreement at any time upon giving the other Party one month's notice in writing of its intention to do so.'

The trust/hospital as the controller has ownership rights to the personal data assigned to that trust/hospital, and a data extract will be securely provided by the Perinatal Institute to the controller upon request if the contract is terminated.

Data is stored for the standard medico-legal requirement of 25 years and an audit trail of all actions are logged. Where the GROW 2.0 record is produced via the GROW 2.0 API, the maternity information system also logs all activity in the audit trail.

4.8 | Lawful Basis for Processing / Necessity and Proportionality

The Perinatal Institute's legal basis for processing personal data:

- UK GDPR - Article 6(e) - Public Interest
- UK GDPR - Article 9(h) - Health or Social Care
  DPA 2018 - Schedule 1, Condition 2, Section 2(c) and 2(d)

The Perinatal Institute as a processor, reference UK GDPR Article 6(e) and Article 9(h) UK GDPR for the lawful basis for processing data on behalf of the controller, so that the controller can provide care. Implied consent and/or affirmative action is referenced by controllers to provide care under the same or additional articles to 6(e) and 9(h). GROW assists clinicians throughout pregnancy, birth, and the postnatal period.

Article 6(e) – Public Interest, the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
Article 9(h) – Health or social care with a basis in law under Schedule 1, Condition 2 of the Data Protection Act 2018 the condition is met under 2(c) and 2(d).

Schedule 1 Data Protection Act 2018 conditions:
Health or social care purposes:

2(1) This condition is met if the processing is necessary for health or social care purposes.
(2) In this paragraph "health or social care purposes" means the purposes of—
(c) medical diagnosis,
(d) the provision of health care or treatment,

NHS England provide a full data controller summary:
england.nhs.uk/contact-us/privacy-notice/nhs-england-as-a-data-controller/

4.9 | Special Category Data

The Perinatal Institute process special category data (ethnicity and health data) under:

- UK GDPR - Article 6(e) – public interest (see section 4.8 for further information)
- UK GDPR - Article 9(3) and DPA 2018, section 204
- UK GDPR - Article 9(h) – Health or Social Care and DPA 2018, Schedule 1, Condition 2, 2(c) & 2(d)
- UK GDPR - Article 9(2)(j) - archiving purposes in the public interest, scientific or historical research or statistical purposes.

UK GDPR Article 6(e)
Lawful basis for processing special category data includes Article 6(e) for the same basis and purpose highlighted in section 4.8. Ethnicity and health data is required as a mandatory data type to assist the controller in providing care.

UK GDPR Article 9(3)
Processing of special category of data includes Article 9(3). Data is being processed by or under

the responsibility of a professional who is subject to an obligation of professional secrecy. DPA 2018, Section 204 provides definitions of the professionals.

UK GDPR Article 9(h)
The Perinatal Institute on behalf of the controller, processes ethnicity and health care data under the lawful basis Article 9(h) for health or social care. Under DPA 2018, Schedule 1, Condition 2 is met under 2(c) and 2(d). The Perinatal Institute keep, review, and maintain an APD (appropriate policy document) detailing special category data information, to comply with UK GDPR.

UK GDPR Article 9(2)(j)
The Perinatal Institute process special category data (ethnicity) for the purpose of fully anonymising data for research, to assist with providing clinical care. This is processed under Article 9(2)(j) - historical research purposes or statistical purposes in accordance with Article 89(1).

From the DPA 2018, Schedule 1, Condition 4 is supported through a Data Anonymisation Policy. Article 89(1) safeguards are also strictly implemented through a Data Anonymisation Policy. This policy can be provided upon request.

NHS England provide a full data controller summary:
england.nhs.uk/contact-us/privacy-notice/nhs-england-as-a-data-controller/

4.10 | Data Processing Agreement

The Perinatal Institute is a processor of personal data. Therefore, a data processor agreement is mandatory between the Perinatal Institute (processor), on behalf of the controller (trust/hospital and sometimes the MIS/API integration party).

A data-sharing agreement may also be sufficient but will need to clearly outline UK GDPR responsibilities in relation to processing activities of the processor and controllers.

4.11 | Rights to Individuals

The controller (trust/hospital) takes primary responsibility for individual rights as they are responsible for providing care. Should an individual make such a request in relation to GROW directly to the Perinatal Institute, the Perinatal Institute will inform the controller and handover/assist the request where necessary. The controller can also make a support request through the Perinatal Institute helpdesk system if assistance is needed.

These rights include:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure/to be forgotten
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

4.12 | Processing for Research Purposes

The Perinatal Institute process, for research purposes, personal and special category data in order to fully anonymise data using the following ICO Codes of Practice (2012):
ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf
ico.org.uk/media/about-the-ico/consultations/2619862/anonymisation-intro-and-first-chapter.pdf

Article 6(4) requires the controller to ascertain whether processing for another purpose is comptatible with the initial purposes the data is collected for. Recital 50 of GDPR and Recital 50, Article 5(1)(b) in the context of research also supports this. Research is mandatory to maintain high levels of clinical accuracy within GROW 2.0.

This research is done for the primary purpose (to provide improved care) to the benefit of the controller(s).
See section 4.3 and 4.9 for further information

The controller(s) instruct the Perinatal Institute to produce an anonymised version of the data as per the anonymisation process and data set fields, for the purposes of: statistical analysis, audit of the database, evaluation of the effectiveness and improvement of the service.

5 | Screening Questions

Screening questions for the inception of the project were analysed, intended to assist in deciding whether a DPIA is necessary for this project.

Question	Answer
Under Article 35(1) – Is this project likely to result in high risk to the rights and freedoms of individuals? Further details here: ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/when-do-we-need-to-do-a-dpia/	**As a data processor (Perinatal Institute):** Yes, Under rare circumstances of Article 35(4) a data breach of personal patient data could lead to *'Risk of physical harm: where the processing is of such a nature that a personal data breach could jeopardise the physical health or safety of individuals. See the first question/answer in section 5 above.'* An example could be: A mother is confidentially pregnant that has a relationship with a domestic abuser. Mother purposely keeps this confidential from an abusive partner. Data breach occurs which could lead to a domestic abuse situation, should the abuser discover this information.
Does the project involve the collection of identifiable information about individuals?	**As a data processor (Perinatal Institute):** Yes, also includes processing, storing, manipulation and transfer (securely).
Does the project require individuals to provide information about themselves or others?	**As a data processor (Perinatal Institute):** Patients – No, they do not provide information about themselves directly to the Perinatal Institute as they do not provide care. Patients provide it to the controller. NHS Professionals – Yes. NHS professionals need to provide contact details to the Perinatal Institute. **Controller's perspective (Trust/Hospital):** From a controller's perspective, yes - individuals provide information for care purposes. Various care professionals would likely analyse this data to provide care. If a patient was to mistakenly submit a request e.g., right to rectification to the Perinatal Institute with their identifiable information, data would only be processed on behalf of the controller, after informing/discussing this with the controller prior to them agreeing to this. This scenario is not a requirement by individuals to provide information about themselves/others.
Will information collected on individuals be available to another person, despite any agreements in place?	**As a data processor (Perinatal Institute):**

	Yes – on behalf of the controller so they can provide care. A data processing agreement should clearly establish this.
Does the project involve the use of technology that might be a high risk to the intrusion of privacy e.g., biometrics?	**As a data processor (Perinatal Institute):** No
From the list of ICO defined high-risk processing operations here: ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/when-do-we-need-to-do-a-dpia/ List any items that apply.	Risk of physical harm: see the first question/answer above in section 5 for a detailed explanation.
Is the project designed to result in providing clinical care, either in the decision or providing increased clinical information that could impact the individual being cared for?	Yes
Does the project involve any data concerning vulnerable individuals who may be unable to easily consent or oppose the processing, or exercise their rights? This group may include children, employees, mentally ill persons, asylum seekers, or the elderly, patients, and cases where there is an imbalance in the relationship between the position of the individual and the controller.	No – This is also at the discretion of the controller (not relevant as a processor).
Is all personal data processed/stored required – could the PID be anonymised or pseudonymised instead?	All personal data is required to provide accurate information. Specific data items are encrypted for protection. For research purposes, data is anonymised.
Is it likely the Perinatal Institute is a controller, joint controller or processor?	Processor only
Based on previous answers, is it likely a DPIA is required?	Yes – mandatory.

6 | Consultation Process

As per all of the Perinatal Institute services, GROW 2.0 undergoes regular comprehensive consultation and upgrades following feedback and national guidance. Within each GAP site, there is a local GAP team consisting of a senior midwife, obstetrician/fetal medicine lead, ultrasonographer, and where appropriate IT. This local GAP team assist with the implementation and ongoing support for the project as well as serving as conduits for regular communication and feedback on the GAP programme and the software to ensure GROW continues to fulfil requirements for clinicians, managers, and mothers.

When communicating with relevant stakeholders, the Perinatal Institute internally would bring this to the relevant IG, Technical, and Clinical teams to form a communication plan.

7 | Governance

The Perinatal Institute Governance summary can be found here: perinatal.org.uk/information/ig

ISO27001

The Perinatal Institute is ISO27001 certified through the BSI (a government-accredited body)

Clinical Risk Register/Clinical Safety Cases

As part of DCB0129 and DCB0160, the Perinatal Institute keeps an up-to-date clinical risk register.
We can provide a copy of this upon request. Further information can be found here: perinatal.org.uk/information/dtac

Cyber Essentials

Certified through Aristi - scope covers the Perinatal Institute entirely.
Certification number: IASME-CE-004397A001

DSP Toolkit

Compliance with DSP Toolkit through NHS - more information here: dsptoolkit.nhs.uk

ICO

Information Commissioners Office registered (No ZA041241; see ico.org.uk/ESDWebPages/Entry/ZA041241) and adhering to all ICO guidelines, including data breach legislation.

Medical Device

GROW 2.0 is a medical device – further information here: perinatal.org.uk/information/dtac

8 | Risk Assessment and controls

Scoring Matrix:

Severity	Catastrophic	5	10	15	20	25
	Major	4	8	12	16	20
	Moderate	3	6	9	12	15
	Minor	2	4	6	8	10
	Negligible	1	2	3	4	5
		5-Yearly	2-Yearly	Annually	Monthly	Weekly
				Likelihood		

Action Matrix:

Risk Rating		**Acceptance Requirements**
Low	1-6	Risks can be accepted by risk owners.
Medium	7-15	Must be reviewed by the IG/ISMS team and can be accepted by them.
High	16-25	Must be reported to SIRO, Director, ISMS Lead, Data Protection Officer. They will review the risk and accept if appropriate

Likelihood of Risk Occurring	
1	5-Yearly – Likely to occur once every 5 years.
2	2-Yearly – Likely to occur once every 2 years.
3	Annually – Likely to occur once every year.
4	Monthly – Likely to occur monthly.
5	Weekly – Likely to occur weekly.

Severity of Impact	
1 – Negligible	**Service:** Brief disruption to service for less than 1 hour, that could have a financial cost of less than £500. **Resources:** Minimal impact on time / costs / resources / projects / staff / reputation / organisation. **Data/IG Implications:** None/no impact **Clinical/patient Safety:** Minimal injury requiring no/minimal intervention or treatment. No time off work required
2 – Minor	**Service:** Loss of service for 1-6 hours that could have financial cost of £500 to £1000. **Resources:** Controllable (minor) impact on time / costs / resources / projects / staff / reputation / organisation. **Data/IG Implications:** Low impact that trigger internal review **Clinical/patient Safety:** Minor injury or illness requiring minor intervention. Requiring time off work for <3 days. Increase in length of hospital stay by 1-3 days
3 - Moderate	**Service:** Loss of service for 6 hours to 3 days that could have a financial cost of £1000 to £5000. **Resources:** Moderate impact on time / costs / resources / projects / staff / reputation / organisation. **Data/IG Implications:** Low/Medium impact that may trigger internal investigation **Clinical/patient Safety:** Moderate injury requiring professional intervention. Requiring time off work for 4- 14 days. RIDDOR / agency reportable incident. An event which impacts on a small number of patients
4 – Major	**Service:** Major loss of service for 3 to 7 days that could have a financial cost of £5000 to £10,000. **Resources:** Major impact on time / costs / resources / projects / staff / reputation that effect the whole company. **External:** Major local news / reputation damage **Data/IG Implications:** High impact with internal investigation - where ICO declaration may be necessary with review **Clinical/patient Safety:** Major injury leading to long-term incapacity/disability. Requiring time off work for >14 days. Increase in length of hospital stay by >15 days. Mismanagement of patient care with long-term effects
5 - Catastrophic	**Service:** Critical loss of service for more than 7 days that could have a financial cost of £10,000 or more. **Resources:** Could impact on the company existing. **External:** Catastrophic **Data/IG Implications:** Severe impact where ICO declaration will be necessary. Could have serious legal repercussions. **Clinical/patient Safety:** Incident leading to death. Multiple permanent injuries or irreversible health effects. An event which impacts on a large number of patients

Risk	Threat	Control(s) Implemented	Controlled Risk Rating	Measure Approved?	Control Outcome
High-risk data processing to individuals has been identified	Under UK GDPR – the risk of physical harm can occur when processing data highlighted in Section 5, in the first table row. If this threat is not effectively controlled, it could lead to a very serious data breach with significant legal implications. It could also lead to physical harm to an individual. Further information: Under rare circumstances of Article 35(4) a data breach of personal patient data could lead to *'Risk of physical harm: where the processing is of such a nature that a personal data breach could jeopardise the physical health or safety of individuals. See the first question/answer in section 5 above.'*	GROW 2.0 has been designed so that controllers (trusts/hospitals) solely provide direct care when using GROW 2.0. This allows care to be provided by trained professionals where trusts/hospitals can decide on and follow correct processes and guidelines to ensure patient confidentially at the level of direct care. High levels of security measures have been implemented throughout GROW 2.0, where a full list of documentation can be found here: perinatal.org.uk/grow2.0/ Some brief examples include HTTPS encryption using RSA 2048 bit, network segregation using VPC's, database encryption, specific data type encryption, infrastructure admin login requires MFA etc. GROW 2.0 has been designed by a range of professionals including a diverse clinical team, that can perform clinically based risks/hazards risk assessments of which physical harm under Article 35(4) is relevant. These types of clinical hazards are reviewed regularly, controls developed then built into GROW 2.0 as ongoing development. Infrastructure supplier AWS (Amazon Web Services) has been vetted under ISO27001 and is a trusted supplier. Services provided are set up and maintained by the Perinatal Institute including security measures. GROW 2.0 user accounts have minimum complexity requirements consisting of 14 characters, requires at least 1 uppercase character, including a mix of alphabetical, numerical, and special characters. This protects against unauthorised access to user accounts, potentially leaking personal data.	Risk Rating: 10 Likelihood: 2 Severity: 5	Yes	Mitigated

Processing special category data	Special category data under UK GDPR requires additional protection or considerations because it's classed as a higher level of sensitive data. To lawfully process special category data, these extra measures must be demonstrated effectively.	Section 4.9 and part of 4.8 effectively justify the means for processing special category data, which includes both Article 6 and Article 9. The Perinatal Institute maintains an APD (appropriate policy document) for processing special category.	Risk Rating: 4 Likelihood: 1 Severity: 4	Yes	Mitigated
UK GDPR	In order to comply with UK GDPR, a significant number of processes, measures, precautions, articles, guidelines, and information needs to be provided or put in place to effectively be compliant. All items related to this must also be kept up to date. Not complying with this could lead to serious issues related to data, that could have legal consequences.	ICO GDPR guidelines and checklist are closely followed and monitored related to GROW 2.0 – further information here: ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data The Perinatal Institute appoint an IG team that form part of a wider steering group, to discuss IG matters between a range of different professionals/specialists within the company. The Perinatal Institute is ISO27001 accredited by an approved government regulatory body, where law and legislation is a key factor. The ISO27001 scope covers the entire company, which includes GROW 2.0.	Risk Rating: 5 Likelihood: 1 Severity: 5	Yes	Mitigated
Infrastructure/network security and data security	Personal data is collected, processed, stored, manipulated, and transmitted. An insecure infrastructure could lead to serious data breaches at multiple levels. Risk to privacy, individuals, compliance and organisational. Additionally, insecure infrastructure security could lead to malicious damage to applications/data through	Application is protected via login authentication. Infrastructure is hosted with AWS using up to date security technologies. All AWS elevated permission accounts require MFA to login. Server ports are all closed by default – and only required protocols are opened.	Risk Rating: 5 Likelihood: 1 Severity: 5	Yes	Mitigated

	unauthorised access. The application could be taken offline.	A full summary of Information Governance standards incorporated into GROW 2.0 is available here: perinatal.org.uk/GROW2.0/ A multi-disciplinary team from a variety of areas which includes a clinical safety case for GROW 2.0. At the clinical level GROW 2.0 including an individual centile calculator hosted separately is also available under disaster recovery circumstances. RDS database is encrypted.			
Development good practices and security requirements	GROW 2.0 will benefit from ongoing development to make improvements in a variety of areas. These updates could also introduce new risks, e.g., a security vulnerability that could lead to a data breach.	The full process and development cycle has been implemented across the whole GROW 2.0 project to effectively ensure new developments to GROW 2.0 are secure, where the security of data is always a key component of this process. This allows for all specialists including IG, clinical, development, infrastructure, security, admin, design, technical, testing to be involved in the ongoing development of GROW to ensure safety measures are taken to prevent this threat.	Risk Rating: 4 Likelihood: 1 Severity: 4	Yes	Mitigated
Service outage/unplanned downtime	These outages could cause data used for clinical care to become unavailable for a period of time. By not being able to use GROW, it's likely a poorer quality of maternity care might be provided.	SLA is a requirement between parties to use the application. The Perinatal Institute guarantee levels of service, also include helpdesk system. See SLA for further information. Infrastructure is hosted on a tested and proven platform within AWS to severely reduce the risk of a technical outage. In the scenario of service outage, alternative GROW 2.0 disaster tool provided as part of SLA hosted on separate servers for emergency scenarios.	Risk Rating: 6 Likelihood: 2 Severity: 3	Yes	Mitigated

		Full disaster recovery and business continuity plans are in place.			
Support requests not serviced in a timely manner	The most serious threats include: • Not being able to access GROW and data/information within e.g., technical error • Incorrect data entered that cannot be changed using the front-end by the clinical user could cause the integrity of data/information to be reduced. • Potential breach of SLA, if service response times are specified within SLA or other type of agreement.	SLA is mandatory between both parties which details support information through helpdesk, including response and resolution times. The helpdesk system is a comprehensive system that has also been reviewed as part of the clinical safety team.	Risk Rating: 6 Likelihood: 2 Severity: 3	Yes	Mitigated
Data breach	Could cause leakage of patient identifiable data or malicious modification of data. Could also cause serious damage to reputation and potentially incur legal costs. Could also potentially lead to physical harm highlighted in Section 5 - Screening.	The Perinatal Institute is registered with ICO (for GDPR) meaning breach reporting is mandatory should it occur which allows the parties involved to be clearly and concisely informed, so that action plans can be put in place. Additionally, a set of standards are implemented here: https://perinatal.org.uk/information/ig to further mitigate this risk. ISO27001 ISMS in particular helps reduce the likelihood of this happening.	Risk Rating: 10 Likelihood: 2 Severity: 5	Yes	Mitigated
Unauthorised access to AWS (infrastructure management platform) or GROW server.	Could cause leakage of data or malicious modification of data. Could also cause serious damage to reputation and potentially incur legal costs. Additionally, service could be tampered with and made unavailable.	Advanced modern security technologies implemented in infrastructure and development of the GROW 2.0 application – see technical specification for further explanation. Some examples include: • Encryption • Network segregation (VPC's) • Authentication • Code reviews	Risk Rating: 5 Likelihood: 1 Severity: 5	Yes	Mitigated

		• Internal & external penetration testing • AWS MFA for privileged users • Advanced log monitoring Full database backups are taken regularly.			
Unauthorised access to Database	Could cause leakage of patient identifiable data or malicious modification of data. Could also cause serious damage to reputation and potentially incur legal costs. Additionally, service could be tampered with and made unavailable.	The database is locked down to a VPC where only authorised remote access controlled through security groups is available. By default, all remote access protocols are revoked. The only way to access the database would be through root/global admin-level access in AWS which has MFA enabled. Root logins are not used, instead, IAM logins are instead created with 'need to have' permissions only.	Risk Rating: 5 Likelihood: 1 Severity: 5	Yes	Mitigated
Transferring information to external media e.g., printing a chart with sensitive information	Transferring data/information to other means of media causes increased methods for it to be maliciously accessed. Increased the risk of a data breach.	The Perinatal Institute protects access to data/information in GROW 2.0 through login authentication. As this is a clinical system (medical device) – the trust/hospital is responsible for direct care (as a controller) of the patient and responsibilities to ensure proper procedures are followed regarding external media. The Perinatal Institute for example cannot prevent someone from taking a photo of the data after logging in, or screenshotting and printing it out.	Risk Rating: 10 Likelihood: 2 Severity: 5	Yes	Transferred
Misuse of the system by end-user	Clinical risk by entering incorrect data or following incorrect procedures.	GROW 2.0 is part of the GAP Programme. As part of the GAP Programme, the Perinatal Institute advise for it to be mandatory for trusts/hospitals to go through E-Learning training at least once annually, which provides all clinical safety guidelines/information/training for using the GROW application correctly. This is part of the GAP SLA between both parties – the Perinatal Institute provides the training E-Learning platform and trusts/hospitals ensure training is kept up to date. Access to the system is only granted once training is completed with a 100% pass score.	Risk Rating: 10 Likelihood: 2 Severity: 5	Yes	Transferred

Potential ICO involvement (Information Commissioner's Office)	If high-risk processing to individuals is identified where it's likely to occur, the ICO should be informed. If ICO determines processing is a too high risk, it could cause the project to cease progress entirely. Not informing ICO when high-risk processing takes place, or not doing an effective DPIA could also lead to legal repercussions.	Risk assessment highlights that although high-risk data to individuals being processed, as it's unlikely to occur then informing ICO is not required. This is due to the risk assessment not containing any unmitigated or dangerous levels of risks within this DPIA.	Risk Rating: 5 Likelihood: 1 Severity: 5	Yes	Mitigated
GROW 2.0 API – Transfer of personal data	As explained in section 4.2 – GROW 2.0 sends personal data back to the call creator, as a return call. Personal data is being transferred which creates additional data risks.	As explained throughout this risk assessment and DPIA, strict security measures have been put in place across all of GROW 2.0 to help protect this data in transit and at rest. The personal data gets sent back to the call creator only as a return call as a JSON file with encryption. If the controller decides to involve a third-party with API integration explained in section 4.2, item 2 – additional risks for the controller(s) may be created – but up to the trust/hospital how they manage this risk.	Risk Rating: 5 Likelihood: 1 Severity: 5	Yes	Mitigated

9 | General Information and Statements / FAQ

Product name: GROW 2.0
GROW 2.0 includes both the GROW 2.0 App and GROW 2.0 API as part of the GAP Programme.

Lawful basis for the processing of personal data:
UK GDPR - Article 6(e) - Public Interest
UK GDPR - Article 9(h) - Health or Social Care: DPA 2018 - Schedule 1, Condition 2 of DPA 2018, section 2(c) and 2(d)

Lawful basis for processing special categories of personal data:
UK GDPR - Article 6(e) - Public Interest
UK GDPR - Article 9(3) - DPA 2018 - Section 204
UK GDPR - Article 9(h) - Health or Social Care
DPA 2018 - Schedule 1, Condition 2 of DPA 2018, section 2(c) and 2(d)
UK GDPR - Article 9(2)(j) - Archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

Section 1 – Data flows and purpose	
Consideration	**Statement**
Perinatal Institute contact information	**SIRO/IG Lead:** Adam Marsters **Data Protection Officer:** Daniel Mallin **Telephone:** 0121 6070101

	Email: ig@perinatal.org.uk
Is PID (personally identifiable information) being processed – could an individual be uniquely identified with the information processed?	Yes – PID is processed to provide care. Yes – An individual can be uniquely identified.
Is all personal data processed/stored required – could the PID be anonymised or pseudonymised instead?	All personal data processed and stored is required. The fundamental purpose of GROW 2.0 is to provide the tools to enhance the safety/quality in providing care. Without processing all data types, this would not be possible. Explained further in Section 4.
Section 2 – Special category data	
Consideration	**Statement**
Is special category data under GDPR Article 9 being processed?	Yes – for providing care • Ethnicity • Health information
Section 3 – Conditions of consent	
Consideration	**Statement**
Statement on consent	The responsibility for consent falls with the controller (trust/hospital) as they provide care under implied consent through common law, and/or affirmative action through UK GDPR. This also includes UK GDPR Individual Rights. The Perinatal Institute does not provide direct care, they provide the GAP Programme and the tools (GROW) to providers to enhance the safety/quality of their care.
Section 4 – Information security	
Consideration	**Statement**
Is information being processed or sent electronically?	Yes – GROW 2.0 (both App and API) is a web application/API hosted online with AWS (Amazon Web Services) over HTTPS. The server and database are located in London, UK also with AWS.
Is data encrypted?	Yes – The network is encrypted over HTTPS with 2048Bit RSA. The database is encrypted through AWS with 256bit AES encryption. EBS (virtual disk) is encrypted with 256bit AES encryption. All data backups in AWS S3 and RDS Snapshots are encrypted with 256bit AES.
Who will access (including any third parties) to any personal data?	The Perinatal Institute – Access to personal data including patient data to perform processor tasks on behalf of controller e.g., to perform data change requests. The Perinatal Institute will not access personal information outside its legal processing activities. Controller (trust/hospital and/or sometimes an MIS/third-party) – access to provide care.

	The Perinatal Institute does not sell, rent, or trade personal data to any third parties. All access to personal data is solely for the purposes of delivering agreed processing services on behalf of the controller. The Perinatal Institute strictly adheres to UK GDPR and ethicalguidelines, and does not use personal data for any purpose beyond those contractually and legally defined.
How long will data be held for?	In line with NHS Records Management Code of Practice: 25 years A pregnancy record is considered as much a part of the child's record as the mother's and therefore any decisions on retention must take this into account. These are the retention schedules as defined by the Records Management Code of Practice: • Childs Record: 25th Birthday • Mothers Record: 25 Years • Clinical Audit: 5 Years after review
Will any PID be stored on portable devices?	No
Information Governance statement on website	https://perinatal.org.uk/information/ig
Section 5 – Third party information	
Consideration	**Statement**
Are you using a third party to process/store PID?	Yes – AWS (Amazon Web Services) Infrastructure is hosted with AWS. AWS are a data processor under UK GDPR terms, but AWS do not take responsibility for what data they process, they just provide the means for others to do so. Infrastructure is maintained by the Perinatal Institute. AWS are a passive data processor only.
Is AWS registered with ICO?	Yes – ZA481902 Further information here: ico.org.uk/ESDWebPages/Entry/ZA481902
How are third parties vetted/reviewed?	The Perinatal Institute compliance review all suppliers as part of ISO27001 complete with full risk assessment. The scope covers the company in its entirety. The Perinatal Institute is ISO27001 accredited and certified through a government-approved body.
Section 6 – Data controller(s) and processor(s)	
Consideration	**Statement**
Who are the data controllers?	The trust/hospital is always the primary data controller. If trusts/hospitals decide to integrate GROW 2.0 (e.g. API) using a third party such as an MIS – the MIS may also be a controller. It's up to Trust/hospital to decide whether they are a joint controller or share primary/secondary UK GDPR responsibilities. This should be reflected in the data processing agreement, or less commonly a data-sharing agreement.
Who are the data processors?	**Data Processing – GDPR** The Perinatal Institute is a data processor on behalf of the controller(s) – trust/hospital and

	sometimes MIS/integration third-party. The Perinatal Institute is a data processor for scenarios such as external support requests made by the trust, where they are the controller. E.g. A trust may request additional information through the helpdesk on a report related to direct care, in this case, the Perinatal Institute would be a processor, to the trust as the controller. The trust/hospital is likely a data processor. If a Trust/hospital integrates with an MIS, they might also be a processor. AWS (hosting supplier) is a data processor under UK GDPR, but passively process in that they provide the infrastructure hosting but don't manage it. AWS would only access the system under legal obligation. Further information here: aws.amazon.com/compliance/data-privacy-faq/

10 | Appendix 1 - Data Items (Full list)

The full list of data types are given below, as a follow on from section 4.5 (all data shown is fake 'dummy' data).

Grow 2.0 Summary Printed: 21/10/2021 Gestation: 34+1

Diana Sample, 11/05/1988,
NHS No. missing, G10002099, BMI 35.9, Parity: 4+0
EDD 01-Dec-2021, Perinatal General Hospital

Mother

Name	Diana Sample
Date of birth	11/05/1988
Parity at booking	4
NHS number	
Chart ID	G10002099
Ethnic Origin	United Kingdom

Antenatal

Plan of Care (last recorded)	Continue current plan
Lead Clinician Role	Midwife

Grow 2.0 Summary Printed: 21/10/2021 Gestation: 34+1

Diana Sample, 11/05/1988,
NHS No. missing, G10002099, BMI 35.9, Parity: 4+0
EDD 01-Dec-2021, Perinatal General Hospital

Booking Details

Maternal height	167
Maternal weight	100
BMI	35.9
Number of babies in pregnancy	Singleton
Antenatal hospital	PI General Hospital
Risk factors (booking)	BMI >=35, P/H SGA / FGR baby, P/H Stillbirth
Plan of care (booking)	Serial EFW scans
Provisional EDD	01/12/2021
Agreed EDD	01/12/2021

Grow 2.0 Summary Printed: 21/10/2021 Gestation: 34+1

Diana Sample, 11/05/1988,
NHS No. missing, G10002099, BMI 35.9, Parity: 4+0
EDD 01-Dec-2021, Perinatal General Hospital

Previous Pregnancies

Details confidential	No
Previous weight at booking	80kg
Number of babies in pregnancy	1
Previous baby DOB	17/12/2019
Gestational age	42+6
First name of previous baby	emily
Outcome	Live birth
Condition since	Alive and well
Sex	Female
Birth weight	3987g
Centile	46.6

Grow 2.0 Summary Printed: 21/10/2021 Gestation: 34+1

Diana Sample, 11/05/1988,
NHS No. missing, G10002099, BMI 35.9, Parity: 4+0
EDD 01-Dec-2021, Perinatal General Hospital

Details confidential	No
Previous weight at booking	85kg
Number of babies in pregnancy	1
Previous baby DOB	17/12/2018
Gestational age	40+0
First name of previous baby	baby 3
Outcome	Stillbirth (24+ weeks)
Condition since	
Sex	Female
Birth weight	2900g
Centile	3.4

Grow 2.0 Summary Printed: 21/10/2021 Gestation: 34+1

Diana Sample, 11/05/1988,
NHS No. missing, G10002099, BMI 35.9, Parity: 4+0
EDD 01-Dec-2021, Perinatal General Hospital

Details confidential	No
Previous weight at booking	80kg
Number of babies in pregnancy	1
Previous baby DOB	17/12/2017
Gestational age	29+0
First name of previous baby	Ella
Outcome	Live birth
Condition since	Alive and well
Sex	Female
Birth weight	2100g
Centile	100

Grow 2.0 Summary Printed: 21/10/2021 Gestation: 34+1

Diana Sample, 11/05/1988,
NHS No. missing, G10002099, BMI 35.9, Parity: 4+0
EDD 01-Dec-2021, Perinatal General Hospital

Details confidential	Yes
Previous weight at booking	85kg
Number of babies in pregnancy	1
Previous baby DOB	17/12/2016
Gestational age	38+6
First name of previous baby	Harvey
Outcome	Live birth
Condition since	Alive and well
Sex	Male
Birth weight	1500g
Centile	0

Grow 2.0	Summary Printed: 21/10/2021 Gestation: 34+1

Diana Sample, 11/05/1988,
, G10002099, BMI 35.9, Parity: 4+0
EDD 01-Dec-2021, Perinatal General Hospital

Investigations

Date	Gest	Investigation	Measurement	Centile	Growth Rate
20-Oct-2021, 20:12	34+0	EFW	nullg		1st EFW < 10th centile
		Doppler	UAD - EDF: EDF reduced UAD - PI: PI/RI normal MCA - RI: PI/RI normal CPR: CPR normal UtAD Notching: - UtAD RI: -		
20-Oct-2021, 19:59	34+0	SFH	34.2cm	N/A	1st plot < 10th
06-Oct-2021, 15:59	32+0	EFW	2000G	45.2	Normal
22-Sep-2021, 15:58	30+0	EFW	1601G	46.1	1st EFW < 10th centile

Diana Sample, 11/05/1988,
, G10002099, BMI 35.9, Parity: 4,
EDD: 01-Dec-2021, Perinatal General Hospital

Mother

Name	Diana Sample
Date of birth	11/05/1988
Parity at booking	4
NHS number	
Chart ID	G10002099

Antenatal

Hospital responsible	Perinatal General Hospital
Risk factors (booking)	BMI >=35, P/H SGA / FGR baby, P/H Stillbirth
Plan of care (booking)	Serial EFW scans
Additional findings	Not recorded
Plan of care (last recorded)	Continue current plan
SFH measurements	1
Scan EFW | Doppler	3 | 1
SFH referred for ?SGA/FGR	No
SGA according to EFW	Not recorded
FGR according to serial EFWs	Yes
FGR according to Doppler	Not recorded
Lead clinician role	Midwife

Diana Sample, 11/05/1988, , G10002099

Labour & Delivery

Place of birth	Perinatal General Hospital
Onset of labour	Spontaneous
Mode of delivery	Spontaneous vertex
Date & time	20-Oct-2021, 19:21

Baby

Outcome	Live birth
Sex	Male
Gestational age	34+1
Birthweight | Centile	2500g | 48.3 centile

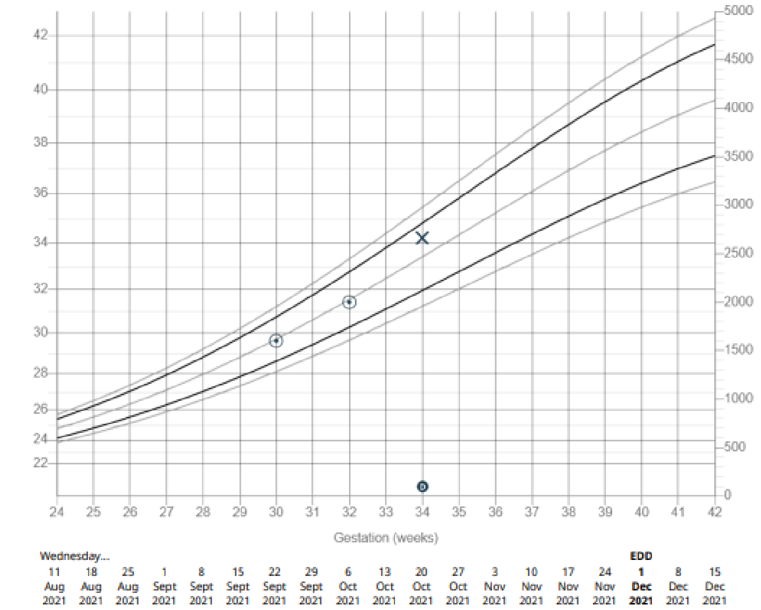
Neonatal

Resuscitation	Basic
Apgar score at 5 mins	4
Birth complications	Birth hypoxia
Transfer to	Neonatal unit

Grow 2.0 This chart was printed on 21/10/2021, 14:25

This chart has been printed from the GROW 2.0 software and may not be up to date

Diana Sample, 11/05/1988,
NHS No. missing, G10002099, BMI 35.9,
Parity: 4, EDD 01-Dec-2021



Date	Time	Gest	Measurement	Signature	Trust