Data Privacy Impact Assessment

FULL DPIA

If a full DPIA is required complete the template below.

Please provide as much information as possible; the ICT Change Control Board is not able to carry out research on your behalf.

DPIA Cover sheet

ICT Help Desk Change Number		
Project / Change Name		**GDm App – Diabetes in Pregnancy**
Requester	**Name**	**< Redacted>**
	Title	**IT Midwife**
	Email	**< Redacted>**
	Phone	**< Redacted>**
Key Stake Holder (organisations) – Name		**ESTH**
	Role	
	Title	
	Email	
	'Phone	
This DPIA will be kept under review by Information Asset Owner	**Name**	**Divisional Director of operations / Women and Children's Service**
	Email	**<Email address Redacted>**

Full DPIA

Name of Organisations involved in the sharing of information	Information will not be shared in bulk for this stage of the project. Information will be shared as normal with patients and other health care providers as needed.
Contract/Agreement: Describe type of contract.	There is a commercial contract in place with Sensyne Health to provide and support the system.
Background information on the project	GDm – Health (v18.1) is a remote mobile communication system to support patients with gestational diabetes mellitus (GDM); a condition which results in high blood sugar levels in women who are pregnant. The primary purpose of GDm-Health (v18.1) is to enable patients and clinicians to remotely monitor blood glucose (BG) levels and to provide a bi-directional communication system between the patient and their clinician. The patient uses the app to record and view their blood glucose readings. The blood glucose readings can be transmitted directly from the patient's personal glucometer to the app via Bluetooth or Near Field Communication (NFC) protocols. Blood glucose readings can also be entered directly in to the app manually. The patient can communicate with their clinician through a messaging feature. The app also displays general information about self - management of GDM. The website version is visible by the patient's clinician located at the hospital, where they can view the blood glucose readings real - time and can also send a message to the patient about how to optimise their blood glucose level management, based on the readings provided by the patient. The blood glucose readings are displayed using colour coding to indicate whether they fall below, within, or above the National Institute for Health and Care Excellence (NICE) guideline thresholds for GDM. The software does not diagnose or otherwise analyse or make clinical interpretations on the blood glucose data, other than to display the results using colour - coding for both individual values and trending of results over time on a line graph. Clinicians are shown alerts on their desktop for when patients record 3 consecutive out of threshold readings for a meal type (high or low for the prandial tag it is associated with) or have submitted fewer than 66% of required readings.
Benefits of the project	The intended benefits of using GDm-Health (v18.1) are to improve the patient's control of their blood glucose levels and thus reduce the number of visits to clinic alongside improving outcomes for mother and baby.

Identify the conditions for each purpose to satisfy Article 6 and 9 of GDPR
How will these be met?

Purpose	GDPR Article 6	GDPR Article 9
'…for the performance of a task carried out in the public interest or in the exercise of official authority…'	6(1)(e)	
'…medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems…'		9(2)(h)

In many cases the conditions would be
Art 6(1)(e) public function and Art 9(2)(h) health & Social Care

Legal Basis for sharing under the Common Law Duty for Confidence	Sensyne Health will explicitly state within the patient's Terms Of Use to be signed by the patient the right to rectification, erasure, restriction, objection, right to withdraw consent at any time, right to lodge a complaint, how the data will be used, stored and duration of retention. Trust retention will be in accordance with the Records Management Code of Practice for Health and Social Care 2016 or successor guidance.

Lawfulness of the processing	**Y/N**
Processing is required by law	**n**
Processing is required to protect the vital interests of the person	**y**
Is any processing going to be by a not for profit organisation, e.g. a Charity	**n**
Would any processing use data already in the public domain?	**y**
Could the data being processed be required for the defence of a legal claim?	**y**
Would the data be made available publically, subject to ensuring no-one can be identified from the data?	**n**
Is the processing for a medical purpose?	**y**
Would the data be made available publically, for public health reasons?	**n**
Will any of the data being processed be made available for research purposes?	**y**

Data Protection Review

Article 5 of the GDPR requires that personal data shall be:

Review compliance with the Data Protection Principles to ensure changes take account of these and follows a 'privacy by design' approach.

Principle	Compliance
(a) processed lawfully, fairly and in a transparent manner in relation to individuals;	The Trust has a fair processing notice on its Internet facing web site. When patients download the app they are required to go through a registration process which explains how their data will be processed and consent to the processing by Sensyne.
(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;	The data is only processed for the purposes the patients have provided the data for as well as for the management of the service.
(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;	Only the data required to treat the patient is recorded and this data is provided by the patient.
(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;	The data is entered by the patient. The data is produced by the blood glucose monitor and mainly automatically transferred with the option of the patient manually inputting the data. Sensyne Health has designed data validation rules at most data entry input points. This will minimize erroneous input. However, quality of data is to be managed at each data controller's own system i.e. the Clinician has the responsibility to check the data inputted is correct. Adequate training will be provided to clinicians on how to use the system prior to deploying it. Data entry points are by the patients and clinicians. The hospital will have and own an instance of the application and therefore will be responsible to keeping patient records within the system up to date.
(e) kept in a form which permits	Data selected by the clinician will be stored in the

identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;	Trust health record according to the Records Management Code of Practice for Health and Social Care 2016. Regarding data held by Sensyne, Patient identifiable Information (PII) will be retained for the lifetime of GDm-Health as a product with a minimum retention period of 12 months. Sensyne Health's data retention policy for backup and subsequent storage is 12 months. The data is backed up so that if the system crashes and GDm-Health needs to be rebuilt, we have a back-up of data available for use. The back-up files are taken nightly and then saved for 12 months After 12 months they are deleted. This back-up file delete does not affect the live database that is serving the GDm-Health product.
(f) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.	Patient data is processed by Sensyne and data is stored, processed and hosted on a UKFast Data Centre; a secure external data centre based in the UK. UKFast is an NHS/HSCN approved supplier and use UK IL4 Standards. Environment is hosted behind CISCO ASA Firewall on UK Fast. UKFast has the following accreditations: G-Cloud 9, ISO 27018, ISO 27001:2013, ISO 14001:2015, NICEIC Electrical Contractor, Cyber Essentials, PCI Compliance. All network communications are HTTPS secured (TLS 1.2). Data is protected in transit.
Article 5(2) requires that: "The controller shall be responsible for, and be able to demonstrate, compliance with the principles."	GDm-Health will record all activities/interactions performed by Clinicians and Patients. The recorded information will contain anonymised data about the Patient and Clinicians which will enable traceability should there be a need. All the audit information will be encrypted and stored in the Sensyne Health managed environment. Sensyne Health has employed Computer Network Defence to carry out black box penetration testing on the system and RecX to conduct security vulnerability assessment. A contract is in place with Sensyne

Consultation/Stakeholder Engagement

This section of the DPIA outlines:

- The key stakeholders;
- The areas of consultation;
- The method of consultation.

Stakeholder	Areas for consultation	Method of consultation	Outcome/Action
EG. Org Name	*EG: Operational matters relating to the joint care plan, consent issues, Fair Processing arrangement*	*E.G: Local internal meetings / Email*	*E.G: Data flows, NPIA, Information Sharing Agreement, consent model, privacy notice*
ESTH	Governance	Meeting / Phone Call / Email with the IG manager / DPO	Completion of DPIA

Q	Category	Screening question	Yes/No
1.7	Data	Does the change involve new process, policy or significantly change the way in which personal and/or business sensitive data is handled?	y
1.8	Data	Does the change involve new or significantly changed handling of a considerable amount of personal and/or business sensitive data about each individual in a database?	y
1.9	Data	Does the change involve new or significantly change handling of personal data about a large number of individuals?	y
1.10	Data	Does the change involve new or significantly changed consolidation, inter-linking, cross referencing or matching of personal and/or business sensitive data from multiple sources?	y
1.11	Data	Will the personal data be processed out of the U.K and / or EEA?	Y

		Please give details	
	All data is held within the EEA apart from data associated with the **SMS service** that GDmHealth provides. GDm-Health has a feature that allows a clinician to send an SMS to a patient. GDm-Health utilises a service provider called Twilio who are based in the US. In order to provide the SMS service, when required Twillio are sent the patients phone number and the free text content of the message. The transfer of data is subject to a lawful transfer mechanism, including the EU-US Privacy Shield. Patients are able to opt out of this service if they so wish.		
1.12	Exemptions and Exceptions	Does the change relate to data processing which is in any way exempt from legislative privacy protections? e.g. "251" exception	N
1.13	Exemptions and Exceptions	Does the change's justification include significant contributions to public security and measures?	N
1.14	Exemptions and Exceptions	Does the change involve systematic disclosure of personal data to, or access by, third parties that are not subject to comparable privacy regulation?	N

2.1	**Is this a new or changed use of personal and/or business sensitive information that is already collected?**	New/Changed
		Yes, in a paper book.

2.2	What data will be collected?									
	Personal Confidential Data Administration data									
	Forename	X	Surname	**X**	Date of Birth	**X**	Age	**X**	Gender	
	Address		Postcode		NHS No	X	Email Address			X
	Payroll number		Bio Metrics e.g. DNA, Finger prints				Tax, benefit, Pension			
	Telephone Number	Y	Hospital Number			Y				
	Bank, financial or credit card details		Mother's maiden name				National Insurance number			
	Health, adoption,		Child		Safeguardin					

	employment, school, Social Services, housing records		Protection		g Adults			
	Another unique identifier (please specify)	N/A						
	Other data *(Please state):*	Blood sugar reading						
	Sensitive data							
	Racial or ethnic origin	*N*	Political opinion	*N*	Religious belief	*N*		
	Trade Union membership	N	Physical or mental health or condition			N		
	Sexual life	N	Commission or alleged commission of an offence			N		
	Proceedings for any offence committed or alleged					N		
	Will the dataset include clinical data? (please include)	Y (Blood sugar level)						
	Will the dataset include financial data?	N						
	Description of other data collected							
	NA							

	<u>Business sensitive data</u>			
	Financial	**<u>N</u>**		
	Local Contract conditions	N	(National contract conditions are in the Public domain)	
	Decisions impacting:	One or more business function	**Yes/No**	
			Y	
		Across the organisation	Y	
	Description of other data collected			
	No other data to be collected but other departments in the Trust may deploy the application			

2.3	**List of organisations involved in processing the data?** *If yes, list below*	Yes
		Yes

	Name	Data Controller (DC) or Data Processor (DP)?	Completed and compliant with the Data Protection and Security Toolkit
			Yes/No
	ESTH	DC	Yes
	Sensyne Health	DP	Yes (8K382)
	UKFast Data Centere	Subcontractor to Sensyne (DP)	
	Twilio	Subcontractor to Sensyne (DP)	
	Patient	DC	N/A
	Comments on organisations involved in processing the data		
	The patient inputs their own data into the application.		
2.4.	**Has a data flow mapping exercise been undertaken?** *If yes, please provide a copy, if no, please undertake – see Note 4 for guidance*		Yes/No Yes
2.5	**Does the Work involve employing contractors external to the Organisation?** *If yes, provide a copy of the confidentiality agreement or contract?*		Yes / No Yes
	Sensyne employ UKfast Data Centre to host the application back end.		

2.6	**Describe in as much detail why this information is being collected/used?**
	As part of the NHS standard of care, women with GDM are reviewed regularly by a hospital - based team at frequent intervals (typically 1 - 4 weeks), which creates a burden on both the health care system and on the patient. Personal Identifiable Data is collected solely for direct patient care. The data is inputted directly into the application by the patients via the mobile application and the clinicians via the desktop application. To enable the clinician to provide direct patient care to patient, each patient has to be fully identified. The data collected will be shared with the hospital clinicians. Beyond direct patient care, data will be anonymised for analysis and research purposes. The Health and Social (Safety and Quality) Act 2015, which came into effect on 1st October 2015 sets a duty for information to be shared where it facilitates care for an individual and it is legal to do so. This sharing requires the patient to be informed and provide them with an opportunity to object. Sensyne Health will ensure all processes and procedures conform with NHS Information Governance Tool Kit, align with GDPR (an European Regulation and Data Protection Act 2018) which is the UK transposition of the GDPR and Clinical Safety Governance The burden has increased in recent years due to changes in diagnostic thresholds coupled with the increasing weight and age of the average maternal population. This has meant an increase in GDM pregnancies from circa 6% of the maternal population to 16% but with no corresponding increase in clinical resources made available for care management. The intended use of the GDm-Health system is to reduce this burden by providing a means for the hospital team to monitor patients' blood glucose levels in real time, reviewing alerts when readings are out of the expected range, and so reducing the need for regular appointments. Use of the GDm-Health system, previous versions, has been shown to "reduce the number of clinic visits by 26%, and reduce the time spent by clinicians on clerical and administrative tasks by 50%". (1 Mackillop L, et al. JMIR Mhealth Uhealth 2018;6(3):e71) GDm-Health system is intended for use for the purposes of clinician to closely monitor and manage diabetes in pregnancy. It will be used to store and transmit data without modification to the health care team. The BG readings and notes around the meals which the patient eats will be used to manage the GDM of a patient, but the decision of management is clinical and comes from a GDM trained clinician. Therefore, the app is a tool which communicates BG readings to a clinician and they will manage a patient's GDM based on these readings. There is no logic behind the management as it is clinician led. However, there is some logic as to how blood glucose readings are deemed too high or low, as described above and determined by NICE GDM guidelines. Clinicians are alerted on the following basis: 1. Red alert for when 3 or more consecutive meal type readings are high or low 2. Amber alerts for when at least 2 out of threshold readings have been posted within the past 2 days where readings were taken 3. Grey alert when not enough readings are taken or when readings are out of range. Sensyne Health will process the data inputted by the patient and the clinician. Sensyne Health will explicitly state within the patient's Terms Of Use to be signed by the patient the right to

	rectification, erasure, restriction, objection, right to withdraw consent at any time, right to lodge a complaint, how the data will be used, stored and duration of retention. Patients who are ≤18 years old and those who are deemed vulnerable will not be provided access to use the application.		
2.7	**Will the information be collected electronically, on paper or both?**	Electronic	Yes
		Paper	N/A
2.8	**Where will the information will be stored:**		
	Data is stored, processed and hosted on a UKFast Data Centre; a secure external data centre based in the UK. UKFast is an NHS/HSCN approved supplier and use UK IL4 Standards. UKFast has the following accreditations: G-Cloud 9, ISO 27018, ISO 27001:2013, ISO 14001:2015, NICEIC Electrical Contractor, Cyber Essentials, PCI Compliance.		

Overview of GDm-Health Data Storage

The diagram in figure 2 below describes the types and categories of data within GDm-Health system and where they are stored. All databases and storages are hosted on Cloud.

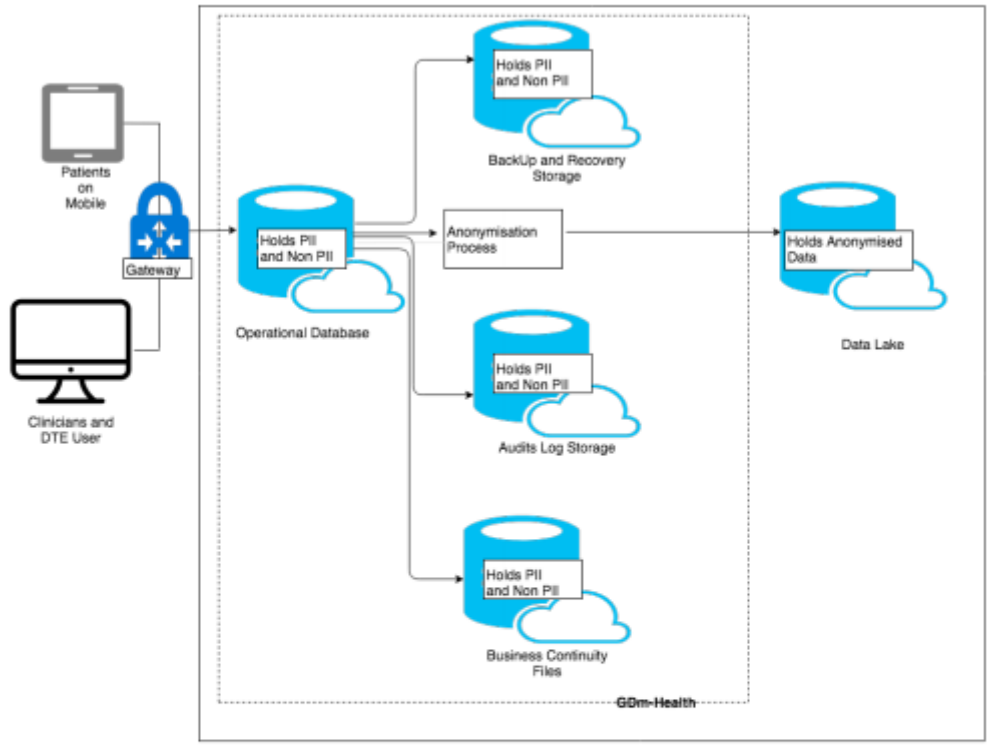

Figure 2: Sensyne Health GDM-Health v18.1.0 Data Storage

1. PII: Personal Identifiable Information
2. Non PII: Non -Personal Identifiable Information
3. Operational Database: This holds and store all the data inputted by patients and clinicians in real time.
4. Backup and Recovery Storage: This holds all backup related data which are taken over night.
5. Audit Log Storage: This holds all information relating to who accessed the system, the action they carried, date and time stamped.
6. Business Continuity Files: This holds PDF version of patient records.
7. Data Lake: This contains anonymised data solely for research and analysis.
8. Anonymisation Process: During the anonymisation process, all personal identifiable are changed in some way such as being removed, substituted, distorted, generalised or aggregated and could be not in any way linked back or reversed.

2.9	**Will this information being shared outside the organisations listed above in question 3?** *If yes, describe who and why:*	No
	No normally.	
2.10	**Is there an ability to audit access to the information?**	Yes
2.11	**What roles will have access to the information?** (list individuals or staff groups)	
	Doctors, Midwives, Patients, Dieticians, Diabetes nurses, Maternity and Health care assistants. The women's health system managers.	

	Sensyne staff will have access to the data as required to support the system.					
2.11	**What security and audit measures have been implemented to secure access to and limit use of personal identifiable and/or business sensitive information?**					
	Username and password	**X**	Smartcard		key to locked filing cabinet/room	
	Secure Token Access		Restricted access to Network Files			
	Is this is a Digital services that maybe attractive to cyber criminals for the purposes of fraud, will the system use transactional monitoring techniques from the outset? Describe below:					Y
	Access is via a gateway in the hosting companies DMZ. A reverse proxy is used to protect the service that accesses the database. The services are containerised for additional security. Technologies used include: 1. Auth0 2. Active Directory or database connector 3. Kong gateway 4. Auth0 signatures 5. Web front-end - a simple web application that perform a login request					
	Other: *Provide a Description Below*:					
	NA					

2.12	**Is Mandatory Staff Training in place for the following?**	Yes/No	Dates
	• Data Collection:	N/A	
	• Use of the System or Service:	YES	Trust staff to be trained then cascade training to other staff as required.
	• Collecting Consent:	N/A	
	• Information Governance:	Yes	EGH staff required to complete annually.
2.13	**Are there any new or additional reporting requirements for this change?**	Y	
	• What roles will be able to run reports?		
	Drs / Midwives login to obtain patient results and produce results		
	• What roles will receive the report or where will it be published?		
	Reports will not normally be distributed by those who run them.		
	• Will the reports be in person-identifiable, pseudonymised or anonymised format?		
	Reports can be identifiable or pseudonymised or anonymised.		
	• Will the reports be in business sensitive or redacted format (removing anything which is sensitive) format?		
	No business sensitive but may be redacted for example for training purposes,		

2.14	**If this new/revised function should stop, are there plans in place for how the information will be retained / archived/ transferred or disposed of?**	**Yes/No**
		Y
	Paper based down time procedure will be used.	
2.15	**Have any Information Governance risks been identified relating to this change?** (if Yes the Risk section below will need to be completed)	Y
2.16	**Are individuals informed about the proposed uses of their personal data?**	Y
2.17	**Are arrangements in place for recognising and responding to requests for access to personal data (SAR)?**	Y
2.18	**Will individuals be asked for consent for their information to be collected and/or shared?** *If no, list the reason for not gaining consent e.g. relying on an existing agreement, consent is implied, he change has s251 approval or other:*	Y

	Yes when using the APP but once data is store in the health record article 9 (2)(h) will be used.	
2.19	How long will data be retained for and How will the data be deleted when no longer required, Please describe below?	
	Trust maternity health records will be retained as per the Records Management Code of Practice for Health and Social Care 2016 (25 years).Data will be stored in the GDM system for 25 years or until the contract with the trust and Sensyne ends. Data will be transferred to the trust in an agreed format. The contract commits ESTH and Sensyne to have a conversion at the termination on how this data should be transferred to ESTH. This is because the most appropriate format in 20 years will be different to the most appropriate format in a years time. All person identifiable information will be anonymised for the purposes of analysis and Research.	

Flow of data within GDm-Health:

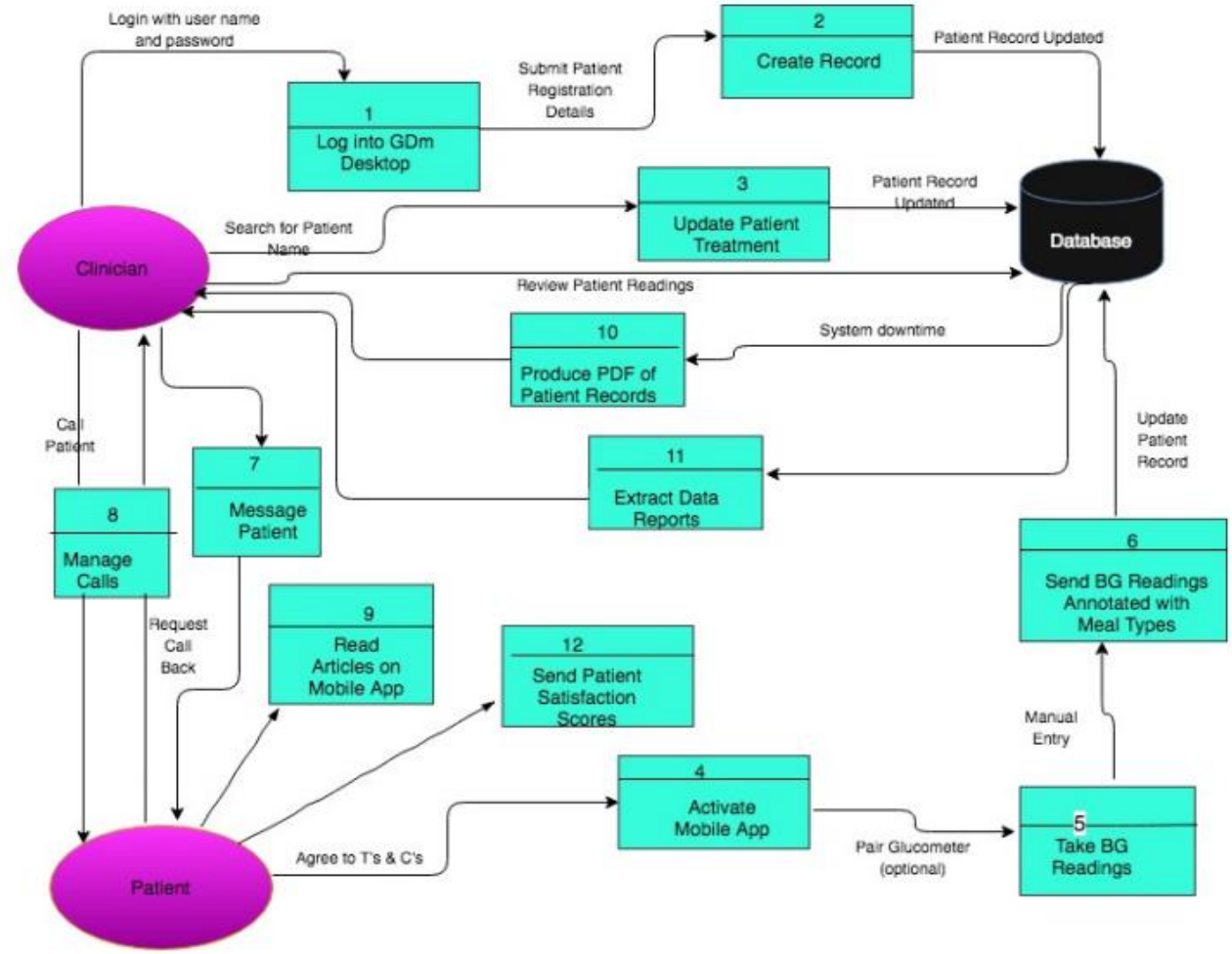

Figure 1: GDm-Health v18.1 .0 Data Flow Diagram

Risks identified and actions required.

Residual risks must be entered onto the Trust risk register.

		Impact				
		1.Trivial	2.Minor	3. Moderate	4. Major	5. Extreme
Probability	1. Rare	Low	Low	Low	Medium	Medium
	2. Unlikely	Low	Low	Medium	Medium	Medium
	3. Moderate	Low	Medium	Medium	Medium	High
	4. Likely	Medium	Medium	Medium	High	High
	5.Very Likely	Medium	Medium	High	High	High

Risk	Probability	Impact	Existing controls:	Result: is the risk eliminated, reduced, or accepted?	Evaluation: is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the change?
Contracting with a sub processor (UK FAST) to host data possess a threat of security breach	Rare	Moderate	The data centre is secure, and the company employs policies and processes to manage staff that mitigate this risk. The platform infrastructure (e.g. distributing data across the solution) make it very unlikely that a malicious party could accurately identify the HDD/SDD that stores the data. Sensyne Health has a contract in place with UK Fast with clauses to cover restrictions, rights to review, audit and monitor the service, process for dealing with any security breaches, service	Reduced	Yes

			termination arrangements.		
Malicious Software Attack	Rare	Extreme	Sensyne Health periodically test the software for all known exploits using in-house and hiring third-party security testing companies. All anomalies are captured and resolved.	Reduced	
Data Sabotage	Rare	Extreme	Sensyne Health hires third-party security testing companies to perform simulated hacking on the application. Data sabotage risk is reduced to ensure that data integrity is prevented.	Reduced	
Human error such as Data Deletion	Likely	Minor	Data deletion cannot be performed by clinicians. They, however, can alter the data e.g. changing patient names etc. Sensyne Health stores audit information of all the changes made to the data entries.	Accepted	
System Malfunction	Likely	Moderate	Sensyne Health's quality testing is very thorough and vigorous to ensure that the system does not malfunction by itself. The system architecture is defined in a manner that isolates unique components and decouple them. This will ensure any malfunction, if it should arise, is limited to the component in question.	Reduced	

Contracting with a sub processor, Twillo, to send text messages to patients registered on the GDm-Health and who have consented to communication via text possess a threat of security breach	Rare	Extreme	Twillo has a stringent and robust Privacy Policy. Sensyne Health has a contract in place with Twillo with clauses to cover restrictions, rights to review, process for dealing with any security breaches, service termination arrangements	Reduced	
Contracting with a sub processor software, Auth0, to enforce user authentication posses a threat of security breach	Rare	Extreme	Sensyne Health has set up very stringent authentication rules which have been technically implemented by AUTH0.	Reduced	

SIGN OFF	
ICT Help Desk Change Number	
Change Name	
Approved by Caldicott Guardian	
Name	**Dr V. De Silva**
Signature	**<Signature Redacted>**
Date	**23-12-19**
Summary of Caldicott Guardian advice:	
Approved by SIRO	
Name	
Signature	
Date	
Summary of SIRO Advice:	
Reviewed by DPO	
Name	**Paul Kenny**
Signature	**<Signature Redacted>**
Date	**23/12/2019**
Summary of DPIO advice:	
Residual risks approved by: If accepting high residual risks consult ICO	
ICT Use only below	

Further Information

Further guidance is available from the information commissioner's web site. The Privacy Impact Assessment Code of Practice provides the relevant templates and further details on how the process should work.

The code of practice can be found at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

References

Data Protection Act 2018
Caldicott principals
Department of Health Information Security Management Code of Practice
NHS Digital
The National Data Guardian's 10 Data Security Standards
https://ico.org.uk/