Data Protection Impact Assessment (DPIA) Template

A DPIA is designed to describe your processing and to help manage any potential harm to individuals' in the use of their information. DPIAs are also important tools for demonstrating accountability, as they help you as a Controller to comply with the requirements of the Data Protection Legislation. Non-compliance with DPIA requirements can lead to fines imposed by the Information Commissioners Office (ICO); this includes not carrying out a DPIA at all, carrying out a DPIA in an incorrect way or failing to consult the ICO where required.

DPIA's are not new; the use of Privacy Impact Assessments has become common practice in the NHS and can provide evidence of compliance within the Data Security and Protection toolkit (DSPT); DPIAs build on that practice.

It is not always clear whether you should do a DPIA or not but there are a number of situations where a DPIA **should** be considered or where a DPIA is a **legal requirement**. If you can tick against the criteria below it is highly recommended that you undertake a DPIA and if you decide not to, ensure that you document the reasons for your decision.

You as Controller **MUST** carry out a DPIA where you plan to:	Tick or leave blank
Use **profiling or automated decision-making** to make significant decisions about people or their access to a service, opportunity or benefit;	✓
Process **special-category data or criminal-offence data on a large scale**;	☐
Monitor a publicly accessible place on a large scale;	☐
Use **innovative technology** in combination with any of the criteria in the European guidelines;	☐
Carry out **profiling** on a large scale;	☐
Process biometric or genetic data in combination with any of the criteria in the European guidelines;	☐
Combine, compare or match data from multiple sources;	☐
Process personal data **without providing a privacy notice** directly to the individual in combination with any of the criteria in the European guidelines;	☐
Process personal data in a way that involves **tracking** individuals' online or offline location or behaviour, in combination with any of the criteria in the European guidelines;	☐
Process **children's** personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them;	☐
Process personal data that could result in a **risk of physical harm** in the event of a security breach.	☐

You as Controller should **consider** carrying out a DPIA where you	Tick or leave blank
Plan any major project involving the use of personal data;	☐
Plan to do evaluation or scoring;	☐
Want to use systematic monitoring;	☐
Process sensitive data or data of a highly personal nature;	☐
Processing data on a large scale;	☐
Include data concerning vulnerable data subjects;	☐
Plan to use innovative technological or organisational solutions;	✓

A new DPIA should be carried out if you decide that there is a significant enough change to what you originally intended but it is good practice for DPIAs to be kept under review and revisited when necessary.

There is guidance to help you. Your Data Protection Officer (DPO) can be consulted before completing a DPIA in order to provide specialist advice and guidance or simply to talk things through with you.

Background Information	
Date of your DPIA :	04/09/2024
Title of the activity/processing:	Heidi Health – AI Scribe software
Who is the person leading this work?	Bret Stevenson – Practice Manager PCHC
Who is the Lead Organisation?	Park Crescent Health Centre
Who has prepared this DPIA?	Mike Cottam – IG Consultant - SCW CSU
Who is your Data Protection Officer (DPO)?	Laura Taw - DPO
Describe what you are proposing to do: (Include as much background information as you can about why the new system/change in system/sharing of information/data processing is required).	Heidi is a healthcare IT system, specifically a cloud-based artificial intelligence medical scribe platform. The system is accessible via desktop and mobile browser for registered users, with servers and data hosted locally in the UK and Ireland. The practice intends to use 'Heidi' to process and transcribe clinical conversations, either between a clinician and patients or of a clinician dictating their clinical findings/management plan during, before or following patient consultations. The technology looks to capture relevant details such as different speakers, medical terminology and symptomatology. The intended purpose behind the technology is to alleviate the administrative burden on healthcare professionals, allowing a greater focus on patient care. Heidi scribe will leverage natural language processing (NLP), speech recognition technology and machine learning algorithms to understand and interpret complex medical dialogue, identify key health information and categorise data into the appropriate sections of an Electronic Health Record (EHR).' 4. Heidi Data Privacy Impact Assessment_N 5. Heidi DTAC Version 1.1 (210624) (
Are there multiple organisations involved? (If yes – you can use this space to name them, and who their key contact for this work is)**.**	Park Crescent Health Centre Heidi Health
Can you think of any other Key Stakeholders that should be consulted or involved in this DPIA? (If so then include the details here).	N/A
Detail anything similar that has been undertaken before?	There is several similar software packages on the market all recently developed and being undertaken with similar timeframes.

1. Categories, Legal Basis, Responsibility, Processing, Confidentiality, Purpose, Collection and Use
1.1.

What data/information will be used? Tick all that apply.	Tick or leave blank	Complete
Personal Data	✓	1.2
Special Categories of Personal Data	✓	1.2 AND 1.3
Personal Confidential Data	✓	1.2 AND 1.3 AND 1.6
Sensitive Data (usually criminal or law enforcement data)	☐	1.2 but speak to your IG advisor first
Pseudonymised Data	✓	1.2 and consider at what point the data is to be pseudonymised
Anonymised Data	✓	Consider at what point the data is to be anonymised
Commercially Confidential Information	☐	Consider if a DPIA is appropriate
Other	☐	Consider if a DPIA is appropriate

1.2.

Processing has to be lawful so identify which of the following you believe justifies what you are proposing to do and include an explanation as to why in the relevant box. You must select at least one from a – f.

Article 6 (1) of the GDPR includes the following:

a) THE DATA SUBJECT HAS GIVEN CONSENT	**Tick or leave blank**
	✓

Why are you relying on consent from the data subject?

Data subjects (patients) will consent to their conversation being recorded but the information that is subsequently transcribed and entered into the clinical record cannot then be deleted unless it is found to be inaccurate. Clinicians will capture consent for this purpose but will not rely on it as their sole lawful basis for processing.

What is the process for obtaining and recording consent from the Data Subject? (How, where, when, by whom).

Describe how your consent form is compliant with the Data Protection requirements? (There is a checklist that can be used to assess this).

N/A

b) IT IS NECESSARY FOR THE PERFORMANCE OF A CONTRACT TO WHICH THE DATA SUBJECT IS PARTY (The contract needs to be between the Controller and the individual and not concern data being processed due to someone else having a contract with the Controller. Processing can happen before the contract is entered into e.g. processing a pre-health assessment for a private or cosmetic procedure that is a paid for service with the delivery of that care done under contract between the Patient and the Practitioner).	**Tick or leave blank**
	☐

What contract is being referred to?

Click here to enter text.

c) IT IS NECESSARY UNDER A LEGAL OBLIGATION TO WHICH THE CONTROLLER IS SUBJECT (A legal obligation mandates processing of data as a task in itself where there are likely to be legal measures available if not adhered to e.g. an Employer has a legal obligation to disclose salary information to HMRC).	**Tick or leave blank**
	☐

Identify the legislation or legal obligation you believe requires you to undertake this processing.

Click here to enter text.

d) IT IS NECESSARY TO PROTECT THE VITAL INTERESTS OF THE DATA SUBJECT OR ANOTHER NATURAL PERSON (This will apply only when you need to process data to protect someone's life. It must be necessary and does not only relate to the individual whose data is being processed. It can also apply to protect another person's life. Emergency Care is likely to fall into this category but planned care would not. You may need to process a Parent's data to protect the life of a child. The individual concerned is unlikely to be able to provide consent physically or legally; if you are able to gain consent then this legal basis will not apply).	**Tick or leave blank**
	☐

How will you protect the vital interests of the data subject or another natural person by undertaking this activity?

Click here to enter text.	
e) IT IS NECESSARY FOR THE PERFORMANCE OF A TASK CARRIED OUT IN THE PUBLIC INTEREST OR UNDER OFFICIAL AUTHORITY VESTED IN THE CONTROLLER (This is different to 6 c). If you are processing data using this basis for its lawfulness then you should be able to identify a specific task, function or power that is set out in law. The processing must be necessary, if not then this basis does not apply).	**Tick or leave blank** ✓
What statutory power or duty does the Controller derive their official authority from? Click here to enter text.	
f) IT IS NECESSARY FOR THE LEGITIMATE INTERESTS OF THE CONTROLLER OR THIRD PARTY (Public authorities can only rely on legitimate interests if they are processing for a legitimate reason other than performing their tasks as a public authority. See the guidance for more information about the legitimate interest test).	**Tick or leave blank** ☐
What are the legitimate interests you have? Click here to enter text.	

Article 9 (2) conditions are as follows:	
a) THE DATA SUBJECT HAS GIVEN EXPLICIT CONSENT (Requirements for consent are the same as those detailed above in section 1.2, a))	**Tick or leave blank** ☐
b) FOR THE PURPOSES OF EMPLOYMENT, SOCIAL SECURITY OR SOCIAL PROTECTION (Schedule 1, part 1 of the Data Protection Act 2018 gives more detail on when this can apply to processing and further guidance is available).	**Tick or leave blank** ☐
c) IT IS NECESSARY TO PROTECT THE VITAL INTERESTS OF THE DATA SUBJECT OR ANOTHER NATURAL PERSON WHERE THEY ARE PHYSICALLY OR LEGALLY INCAPABLE OF GIVING CONSENT (Requirements for this are the same as those detailed above in section 1.2, d))	**Tick or leave blank** ☐
d) It is necessary for the operations of a not-for-profit organisation such as political, philosophical, trade union and religious body in relation to its members	*NA*
e) The data has been made public by the data subject	*NA*
f) For legal claims or courts operating in their judicial category	*NA*
g) SUBSTANTIAL PUBLIC INTEREST (Schedule 1, part 2 of the Data Protection Act 2018 gives more detail on when this can apply to processing and further guidance is available).	**Tick or leave blank** ☐
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 ON THE BASIS OF UNION OR MEMBER STATE LAW OR PURSUANT TO CONTRACT WITH A HEALTH PROFESSIONAL AND SUBJECT TO CONDITIONS AND SAFEGUARDS (Schedule 1, part 1 of the Data Protection Act 2018 gives more detail on when this can apply to processing and further guidance is available).	**Tick or leave blank** ✓
i) PROCESSING IS NECESSARY FOR REASONS OF PUBLIC INTEREST IN THE AREA OF PUBLIC HEALTH, SUCH AS PROTECTING AGAINST SERIOUS CROSS-BORDER THREATS TO HEALTH OR ENSURING HIGH STANDARDS OF QUALITY AND SAFETY OF HEALTH CARE AND OF MEDICINAL PRODUCTS OR MEDICAL DEVICES, ON THE BASIS OF UNION OR MEMBER STATE LAW WHICH PROVIDES FOR SUITABLE AND SPECIFIC MEASURES TO SAFEGUARD THE RIGHTS AND FREEDOMS OF THE DATA SUBJECT, IN PARTICULAR PROFESSIONAL SECRECY (Schedule 1, part 1 of the Data Protection Act 2018 gives more detail on when this can apply to processing and further guidance is available).	**Tick or leave blank** ☐

j)	**PROCESSING IS NECESSARY FOR ARCHIVING PURPOSES IN THE PUBLIC INTEREST, SCIENTIFIC OR HISTORICAL RESEARCH PURPOSES OR STATISTICAL PURPOSES IN ACCORDANCE WITH ARTICLE 89(1) BASED ON 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.** (Schedule 1, part 1 of the Data Protection Act 2018 gives more detail on when this can apply to processing and further guidance is available).	**Tick or leave blank** ☐

1.3.

If using special categories of personal data, a condition for processing under Article 9 of the GDPR must be satisfied in addition to a condition under Article 6. You must select at least 1 from a) to c) or g) to j). NOTE: d), e) and f) are not applicable

1.4.

Confirm who the Controller and Processor is/are. Confirm if the Controller/s are solely or jointly responsible for any data processed?

(Identify any other parties who will be included in the agreements and who will have involvement/share responsibility for the data/information involved in this project/activity. Use this space to detail this but you may need to ask your DPO to assist you. Copy and paste the last empty row in the table to add organisations where required (the text has been left unlocked for this purpose on that row only).

Name of Organisation	Role
Park Crescent Health Centre	Sole Controller
Heidi Health	Processor
Click here to enter text.	Choose an item.
Click here to enter text.	Choose an item.
Click here to enter text.	Choose an item.
Click here to enter text.	Choose an item.
Click here to enter text.	Choose an item.

1.5.

Describe exactly what is being processed, why you want to process it and who will do any of the processing?

Heidi works by transcribing speech into text from a healthcare encounter such as conversations between clinicians and patients or by clinicians dictating their clinical findings, impressions and/or management plans before, during and after the patient consultation. The clinician can also add additional contextual notes about the encounter afterwards which they may not wish to verbalise during.

Once the transcription is created, it undergoes de-identification and pseudonymisation, where identifiable information is either removed or replaced with coded references. At this stage, the Large Language Model (LLM) refines the notes before the final version appears in the web portal. This entire process is highly automated and completed quickly. By the time the notes are stored in the cloud, they are fully de-identified.

No patient-identifiable data is ever shared with third parties (see listed orgs at section 3).

Access to these notes is governed by the principle of least privilege—only authorised personnel, as designated by the clinician, can access the data, and only to the extent necessary for operational or troubleshooting purposes. Heidi itself doesn't handle any patient data directly after it's transferred. To further clarify the process:

- **At the recording stage**, no one has access as the recording is automatically deleted once transcription is complete.

- **During processing**, the data is encrypted in transit and de-identified, and no one outside the authorised team can access those details.
- **Final storage** is entirely controlled by the clinician within their Heidi platform.

Once the document is produced, the clinician then is required to manually copy and paste it into the relevant clinical record. Each document is reidentified at this stage to ensure there is no confusion. A future goal for Heidi Health is to allow for integration with the clinical system (IM1) to negate the need for manual intervention by the clinician. Once this change is available, this DPIA will need to be updated.

The extent of the data that could be recorded and subsequently transcribed extends (but is not limited to): name, address, phone number, gender, sexual orientation, DOB, relationship status, family and social history, medical history, medications and prescriptions, allergies, diagnoses, lab results, disabilities

The clinician will engage with patient and ask for their consent to record and must provide appropriate transparency information at this initial stage.

Pseudonymisation
Pseudonymisation is the process of transforming personal data in such a way that individuals cannot be identified without additional information. This is done by first identifying sensitive data types, including transcripts, patient information, clinician notes, and generated notes. Sensitive data is encrypted both while in transit, and at rest, and all keys are managed securely. Machine learning (ML) techniques are used to de-identify transcript data, targeting entities like names, genders, addresses, emails, and phone numbers. This is done by replacing identifying fields within a data record with artificial identifiers, or pseudonyms. For example, instead of storing a person's name, the data might store a unique code that only authorised personnel can trace back to the original individual. The direct identifiers are extracted and temporarily stored separately within the AWS servers in the UK during this pseudonymisation process. The key to re-identify the data is kept separately and securely by Heidi, ensuring that even if the pseudonymised data is accessed, the privacy of individuals remains protected. However, the entire process takes place automatically via the de-identification model. This technique is crucial for maintaining privacy while still allowing data to be used for analysis and improving ML accuracy.

1.6.
Tick here if you owe a duty of confidentiality to any information. ✓

If so, specify what types of information. (e.g. clinical records, occupational health details, payroll information)
Clinical records

1.7.
How are you satisfying the common law duty of confidentiality?
Consent - Implied

If you have selected an option which asks for further information, please enter it here
Click here to enter text.

1.8.
Are you applying any anonymisation/pseudonymisation technique or encryption to any of the data to preserve the confidentiality of any information?
Yes

If you are, then describe what you are doing.
Identifiable data collected as part of recordings that are made will be de-identified and pseudonymised before the transcript is then processed into any formal clinical documentation.

If you don't know then please find this information out as there are potential privacy implications with the processing.

1.9.
Tick here if you are intending to use any information for a purpose that isn't considered as direct patient care. ☐

If so, describe that purpose.
Click here to enter text.

1.10.
Approximately how many people will be the subject of the processing?
GP Practice population

1.11.
How are you collecting the data? (e.g. verbal, electronic, paper (if you need to add more selections then copy the last 'choose an item' and paste, the text has been left unlocked for you to do this.)
Face to face - in person
Web based data collection
Choose an item.
Choose an item.
Choose an item.

If you have selected 'other method not listed' describe what that method is.
Click here to enter text.

1.12.
How will you edit the data?
Data collected as part of the recording/transcript is subject to review and editing as appropriate by the clinician before any information is added to the clinical record

1.13.
How will you quality check the data?
All outputs generated by the system should be reviewed by a clinician before they are utilised further. Ultimately the clinician is always responsible for the documentation produced and must ensure that the information contained within it is accurate and truly reflects what was discussed during the patient consultation.

Heidi does implement rigorous processes for eliminating biases in outputs produced. This involves continuous monitoring and evaluation of algorithms to detect and mitigate any potential biases that may arise. The approach includes diverse and representative data sets, regular audits, and feedback loops from clinicians to refine and enhance the system.

1.14.
Review your business continuity or contingency plans to include this activity. Have you identified any risks?
No

If yes include in the risk section of this template.

1.15.
What training is planned to support this activity?
N/A

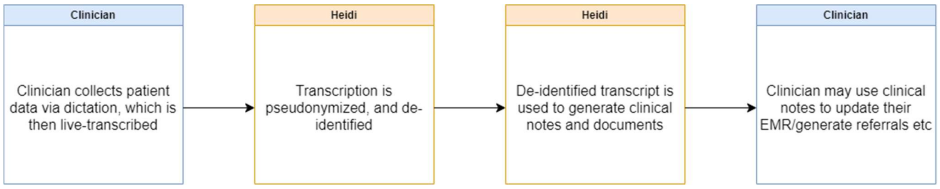
2. Linkage, Data flows, Sharing and Data Opt Out, Sharing Agreements, Reports, NHS Digital

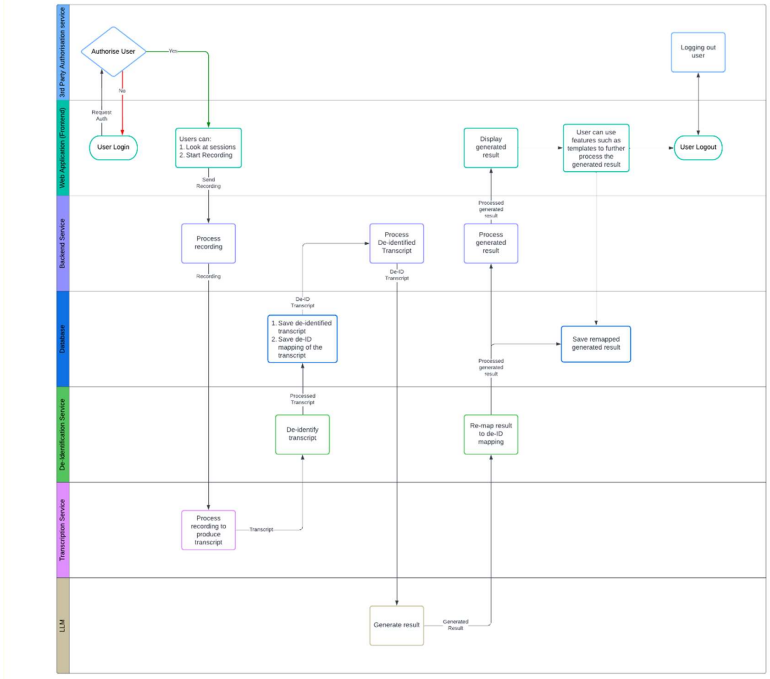
2.1.
Are you proposing to combine any data sets?
No

If yes, then provide the details here.
Click here to enter text.

2.2.

What are the Data Flows? (Detail and/or attach a diagram if you have one).





2.3.

What data/information are you planning to share?

No identifiable patient data is ordinarily accessible to Heidi Health or any sub-processors. Data collected as part of the transcript recording is technically accessible to them (through numerous pseudonymisation keys) but would only be used for troubleshooting purposes.

Heidi has strict data processing agreements with all third parties involved in processing, which are designed to ensure that no user (patient) data can be accessed, used, or stored by third parties beyond that which is necessary for the specific purposes for which it was shared. Zero retention policies are enforced with all providers, thereby ensuring no data is retained, reused or accessed for any additional purposes.

2.4.
Is any of the data subject to the National Data Opt Out?
No - it is not subject to the national data opt out

If your organisation has to apply it describe the agreed approach to this
Click here to enter text.

If another organisation has applied it add their details and identify what data it has been applied to
Click here to enter text.

If you do not know if it applies to any of the data involved then you need to speak to your Data Protection Officer to ensure this is assessed.

2.5.
Who are you planning to share the data/information with?
See section 2.3 above

2.6.
Why is this data/information being shared?
To help streamline the administrative side of documenting patient interactions by clinicians by introducing a degree of automation into the process

2.7.
How will you share it? (Consider and detail all means of sharing)
Clinicians retain ownership of all transcripts, clinical notes and documents that are created as a result of the recordings. No identifiable recordings are stored or will be accessible (except for troubleshooting) by Heidi et al.

Tick if you are planning to use Microsoft Teams or another similar online networking/meeting solution that may have the facility to store or record conversations or related data as part of the sharing arrangements ☐

Provide details of how you have considered any privacy risks of using one of these solutions
Click here to enter text.

2.8.
What data sharing agreements are or will be in place?
A Data Processing Agreement will be necessary between the practice and Heidi Health.

Heidi Health also has a robust set of data processing agreements with each of its sub-processors

2.9.
What reports will be generated from this data/information?
Aggregate de-identified information from patient consultations will be used by Heidi to improve models and outputs, ultimately with the goal of improving patient care and clinician experience.

2.10.
Are you proposing to use Data that may have come from NHS Digital (e.g. SUS data, HES data etc.)?
No

If yes, are all the right agreements in place?
Choose an item.

Give details of the agreement that you believe covers the use of the NHSD data
Click here to enter text.

If no or don't know then you need to speak to your Data Protection Officer to ensure they are put in place if needed.

3. Data Processor, IG Assurances, Storage, Access, Cloud, Security, Non-UK processing, DPA

3.1

Are you proposing to use a third party, a data processor or a commercial system supplier?

Yes

If yes use these spaces to add their details including their official name and address. If there is more than one then include all organisations. If you don't know then stop and try and find this information before proceeding.

Heidi Health Trading Pty Ltd, Level 5, 24-26 Cubitt Street, Cremorne, Melbourne, 3121
Google LLC, 1600 Amphitheatre Parkway, Mountain View, California, 94043 **(data processed within the EU - Ireland)**
Amazon Web Services UK **(data processed within the UK)**
Kinde - Suite 2 Level 5, 6/10 O'Connell St, Sydney NSW 2000, Australia **(data processed within EU – Ireland)**
Stripe **(data processed within the UK)**
Intercom **(data processed within the EU – Ireland)**

3.2

Is each organisation involved registered with the Information Commissioner? Copy and paste the last empty row in the table to add organisations where required (the text has been left unlocked for this purpose on that row only)

Name of organisation	Registered	Registration details or comments if not registered
Hedi Health Trading Pty Ltd	Yes	ZB671518
Google LLC	Yes	Z2451429
Amazon Web Services UK	Yes	ZA481902
Kinde	No	Click here to enter text.
Stripe	No	Click here to enter text.
Intercom	Yes	ZA931797*

3.3

What IG assurances have been provided to you and does any contract contain IG clauses that protect you as the Controller? (e.g. in terms and conditions, their contract, their tender submission). Copy and paste the last empty row in the table to add organisations where required (the text has been left unlocked for this purpose on that row only)

Name of organisation	Brief description of assurances obtained
Heidi Health Trading Pty ltd	ISO27001, Cyber Essentials and SOC2 certifications, Pen testing, DSPT compliant, DTAC, robust DPA in place with GP practice
Google LLC	Click here to enter text.
Amazon Web Services UK	Click here to enter text.
Kinde	Click here to enter text.
Stripe	Click here to enter text.
Intercom	Click here to enter text.

3.4

What is the status of each organisation's Data Security Protection Toolkit?

DSP Toolkit

Copy and paste the last empty row in the table to add organisations where required (the text has been left unlocked for this purpose on that row only)

Name of organisation	ODS Code	Status	Published date
Heidi Health (Australia)	HHA001	23/24 Standards Met	11/04/2024
Google LLC	8JE14	23/24 Standards Exceeded	27/05/2024

Amazon Web Services	8JX11	23/24 Standards Exceeded	18/06/2024
Click here to enter text.	Click here to enter text.	Click here to enter text.	Click here to enter text.
Click here to enter text.	Click here to enter text.	Click here to enter text.	Click here to enter text.
Click here to enter text.	Click here to enter text.	Click here to enter text.	Click here to enter text.

3.5

How and where will the data/information be stored? (Consider your answer to 2.7 and the potential storage of data in any online meeting or networking solution).

No identifiable recordings are stored. Clinicians retain ownership and control over all patient data captured and have the right to access, update and delete all data at their discretion.

Please refer to 1.5 for storage and de-identification details. The extracted identifiers are temporarily held within AWS UK servers as part of the pseudonymisation process before being reinserted to the final clinical document that is produced.

Cloud based servers provided by AWS UK store pseudonymised transcripts and clinical notes only.

Heidi is accessible via desktop and mobile browser to registered users, with servers and data hosted locally in the UK for all UK users.

The clinician retains control over the documents produced and can set their own auto-deletion timers as they see fit.

3.6

How is the data/information accessed and how will this be controlled?

Access to the system is only granted to registered clinician users

Heidi determines the type and level of access granted to its own individual users based on the "principle of least privilege." This principle states that users are only granted the level of access absolutely required to perform their job functions. Permissions and access rights not expressly granted shall be, by default, prohibited. Heidi's primary method of assigning and maintaining consistent access controls and access rights shall be through the implementation of Role-Based Access Control (RBAC).

3.7

Is there any use of Cloud technology?

Yes

If yes add the details here.

Cloud based servers hosted by Amazon Web Services UK

3.8

What security measures will be in place to protect the data/information?

Heidi employs stringent privacy and security measures, including end-to-end and at rest encryption, regular audits, real-time security monitoring, and penetration testing. It holds ISO27001, Cyber Essentials and SOC2 certifications, aligns with GDPR and other international data privacy regulations.

Is a specific System Level Security Policy needed?

Yes

If yes or don't know then you need to speak to your Data Protection Officer to ensure one is put in place if needed.

A SLSP is in place, along with other specific documents governing Heidi's IT processes. The SLSP outlines how we protect data and ensure compliance with industry standards, including access control, incident response, and risk management.

3.9
Is any data transferring outside of the UK? (you must determine this so only select don't know if you have further investigations to make but the DPIA will not be approved without this information)
Yes

If yes describe where and what additional measures are or will be in place to protect the data.
All data is processed within the UK or Ireland

3.10
What Data Processing Agreement is already in place or if none, what agreement will be in place with the organisation and who will be responsible for managing it?

Heidi Data Processing Agreeme

Commented [MC1]: ACTION - Practice to ensure that they implement a Data Processing Agreement with Heidi Health with appropriate IG clauses

4. Privacy Notice, Individual Rights, Records Management, Direct Marketing

4.1
Describe any changes you plan or need to make to your Privacy Notice and your proposed completion date? (There is a checklist that can be used to assess the potential changes required or if you wish for it to be reviewed then add the link below).
GP practice to update privacy notice to ensure it reflects their relationship with Heidi Health and allows patients to be aware of how their data will be processed. May be appropriate to link to Heidi Health's own privacy information for more comprehensive information

4.2
How will this activity impact on individual rights under the GDPR? (Consider the right of access, erasure, portability, restriction, profiling, automated decision making).
Limited impact – patients will still be able to engage with their GP practice should they wish to exercise their individual rights.

4.3
How long is the data/information to be retained?
This processing will occur every time a clinician performs a session on Heidi - in other words, every time they click 'start recording'. This data will cover both data from the patient themselves (though it is de-identified) and the clinician too - such as their templates, note-taking style, clinician type, email address etc. No identifiable recordings are stored or will be accessible. Clinicians retain ownership of all transcripts, clinical notes, and clinical documents and can decide how long this data is stored. They can do this through setting up their own tailored auto-deletion timers which are set to timeframes they deem appropriate. Any and all identifiable information is deleted once this timeframe is reached and will be irretrievable by the clinician and Heidi staff. Additionally, the patient information contained in these transcripts and clinical notes/documents will only be accessed externally for the purpose of troubleshooting with the express permission of clinicians.

By default, the data is set to never delete, but automatic deletion can be scheduled in the user settings for 1, 7, 21, or 90 days, depending on the clinician's preference.

4.4
How will the data/information be archived?
See 4.3

4.5
What is the process for the destruction of records?
No identifiable data retained by any third party. Clinicians can set their own desired retention and have the ability to delete records at any time should they wish

4.6
What will happen to the data/information if any part of your activity ends?
See item 10 of the DPA

Commented [MC2]: Practice to refer to terms set out within Data Processing Agreement

4.7
Will you use any data for direct marketing purposes? (you must determine this so only select don't know if you have further investigations to make but the DPIA will not be approved without this information)

No

If yes please detail.

Click here to enter text.

5. Risks and Issues

5.1

What risks and issues have you identified? The DPO can provide advice to help complete this section and consider any measures to mitigate potential risks.

Describe the source of risk and nature of potential impact on individuals. (Include associated compliance and corporate risks as necessary and copy and paste the complete bottom row to add more risks (the text has been left unlocked in both tables to enable you to do this)).	**Likelihood of harm**	**Severity of harm**	**Overall risk**
Data breach resulting in loss of information	Possible	Significant	Medium
Recording not manually stopped by clinician, rolling over to a consultation with a non-consenting patient	Possible	Significant	Medium
Speech-to-text model fails to accurately transcribe what has been discussed resulting in missed or incorrect treatment for patients	Possible	Significant	Medium
Failure of transparency to patient about being recorded and recording without consent	Possible	Significant	Medium
Practice not creating an SOP to ensure a standard data retention period is set and adhered to.	Possible	Significant	Medium
Manual copying and pasting of documents into patient record by clinician could result in error	Possible	Significant	Medium

Commented [MC3]: ACTION - Practice to consider risks identified, and add in appropriate mitigations

5.2

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in 5.1

Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved (SIRO)**
Data breach resulting in loss of information	Heidi employs stringent privacy and security measures, including end-to-end and at rest encryption, regular audits, real-time security monitoring, and penetration testing. It holds ISO27001, Cyber Essentials and SOC2 certifications, aligns with GDPR and other international data privacy regulations.	Reduced	Low	Yes

Commented [HU4]: GP practice to ensure all risk mitigations are implemented and understood. Caldicott Guardian to review the risks and approve sign off

	As per DPA Heidi Health shall notify the Data Controller without undue delay (and in any event, within 24 hours) upon becoming aware of any data breach affecting Personal Data.			
Recording not manually stopped by clinician, rolling over to a consultation with a non-consenting patient	Train staff to check the recording status before starting a new consultation	Reduced	Low	Yes
Speech-to-text model fails to accurately transcribe what has been discussed resulting in missed or incorrect treatment for patients	Clinician should review and confirm each transcript before they are added to the patients medical records. Appropriate training for clinical staff provided to ensure staff proficient in system	Reduced	Low	Yes
Failure of transparency to patient about being recorded and recording without consent	Practice to implement a clear process for obtaining patients explicit consent before recordings begin. Consent should be recorded whether verbally or explicit. All staff should be trained on obtaining consent and informing patients about the recordings	Reduced	Low	Yes
Practice not creating an SOP to ensure a standard data retention period is set and adhered to.	Practice to create a SOP which includes data retention. Regular audits should also be conducted to ensure the retention period is being adhered to	Reduced	Low	Yes
Manual copying and pasting of documents into patient record by clinician could result in error	Clinician should always double check the information is accurate before saving it in the patients record. All clinicians should be updated with regular training including new clinicians on using Heidi Health responsibly.	Reduced	Low	Yes

5.3
What if anything would affect this piece of work?
Click here to enter text.

5.4
Please include any additional comments that do not fit elsewhere in the DPIA?
Click here to enter text.

6. Consultation

6.1
Have you consulted with any external organisation about this DPIA?
Choose an item.

If yes, who and what was the outcome? If no, detail why consultation was not felt necessary.
Click here to enter text.

6.2
Will you need to discuss the DPIA or the processing with the Information Commissioners Office? (You may need the help of your DPO with this)
Choose an item.

If yes, explain why you have come to this conclusion.
Click here to enter text.

7. Data Protection Officer Comments and Observations

7.1
Comments/observations/specific issues

The practice should establish an SOP for the use of Heidi Health, and this should include a standard retention period across all users within your practice. This should also be included in the practice local retention schedule.

The practice should ensure they update their Information Asset Register and Data Flow Map to include this process.

The practice should update their privacy notice. Suggested wording for Privacy notice.

	Purpose: The practice intends to use 'Heidi' to process and transcribe clinical conversations, either between a clinician and patients or of a clinician dictating their clinical findings/management plan during, before or following patient consultations. The technology looks to capture relevant details such as different speakers, medical terminology and symptomatology. **Legal Basis**: **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" **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" **Processor**: Heidi Health

8. Review and Outcome

Based on the information contained in this DPIA along with any supporting documents, you have determined that the outcome is as follows:
A) There are no further actions needed and we can proceed

If you have selected item B), C) or D) then please add comments as to why you made that selection
Click here to enter text.

We believe there are
Choose an item.

If you have selected item B) or C) then list these in the amber boxes below and then consider additional measures you could take and include these in the green boxes below

Residual risks and nature of potential impact on individuals. (Include associated compliance and corporate risks as necessary and copy and paste the complete bottom row to add more risks (the text has been left unlocked in both tables to enable you to do this)).	**Likelihood of harm**	**Severity of harm**	**Overall risk**
Click here to enter text.	Choose an item.	Choose an item.	Choose an item.
Click here to enter text.	Choose an item.	Choose an item.	Choose an item.
Click here to enter text.	Choose an item.	Choose an item.	Choose an item.
Click here to enter text.	Choose an item.	Choose an item.	Choose an item.

Additional measures you could take to reduce or eliminate residual risks identified as medium or high risk above (B and C)				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved (SIRO)**
Click here to enter text.	Click here to enter text.	Choose an item.	Choose an item.	Choose an item.
Click here to enter text.	Click here to enter text.	Choose an item.	Choose an item.	Choose an item.
Click here to enter text.	Click here to enter text.	Choose an item.	Choose an item.	Choose an item.
Click here to enter text.	Click here to enter text.	Choose an item.	Choose an item.	Choose an item.

Signed and approved on behalf of Park Crescent Health Centre

Name: Bret Stevenson

Job Title: Practice Manager

Signature: B Stevenson Date: 01/03/2025 Signed and approved on behalf of Click here to enter text. Name: Click here to enter text. Job Title: Click here to enter text. Signature: Click here to enter text. Date: Click here to enter a date.
Please note: You should ensure that your Information Asset Register and Data Flow Mapping Schedules are updated where this is relevant. This DPIA can be disclosed if requested under the Freedom of Information Act (2000). If there are any exemptions that should be considered to prevent disclosure detail them here: Click here to enter text.