16 February 2026

Health New Zealand
Te Whatu Ora

[redacted]

Tēnā koe [redacted]

Your request for official information, reference: HNZ00106690

Thank you for your email on 2 January 2026, asking Health New Zealand | Te Whatu Ora for the following under the Official Information Act 1982 (the OIA):

1. *Documents, reports, summary and communications used in the NAIAEAG review process, including any internal processes and meetings involving Heidi AI implementation.*
2. *Copies of any contracts, agreements, or formal arrangements related to the Heidi AI project and its integration into Te Whatu Ora Health NZ.*
3. *Specific details of the implementation plans for Heidi AI, including any timelines, milestones, and resource allocations.*
4. *A summary of the risks identified in relation to Heidi AI, including any risk management or mitigation strategies discussed.*
5. *Records of governance discussions or meetings regarding the Heidi AI project, particularly those addressing oversight, accountability, and ethical considerations.*
I request that you provide these documents in electronic format where possible. If it requires a substantial amount of hours to collate all these, I request key summary documentations that lay out the above points please.

Response

Many clinicians around the country were using Heidi AI Scribe in a clinical setting prior to Health New Zealand's contract with Heidi AI. Health New Zealand's procurement of Heidi AI has ensured that existing use is safer, patient data is secure, and the outputs produced are fit for purpose.

Please refer to **Appendix One,** which sets out our decision on the release of documents within scope of your request. The documents able to be released are attached as **Appendix Two**.

For the sake of clarity, I will address each question in turn and list the relevant document numbers in scope of each part of your request.

1. *Documents, reports, summary and communications used in the NAIAEAG review process, including any internal processes and meetings involving Heidi AI implementation*

We have interpreted "communications" for the purposes of your request as referring to formal communications used as part of the NAIAEAG review process or to inform staff or external stakeholders, such as reports, assessments, briefings, or updates relating to the implementation of Heidi AI. Relevant communications of this nature have been identified as Documents 1 and 3.

2. *Copies of any contracts, agreements, or formal arrangements related to the Heidi AI project and its integration into Te Whatu Ora Health NZ*

Please refer to Documents 9 and 10.

3. *Specific details of the implementation plans for Heidi AI, including any timelines, milestones, and resource allocations*

Please refer to Documents 5, 6 and 7.

4. *A summary of the risks identified in relation to Heidi AI, including any risk management or mitigation strategies discussed*

Please refer to Documents 3, 5, 9 and 10.

5. *Records of governance discussions or meetings regarding the Heidi AI project, particularly those addressing oversight, accountability, and ethical considerations*

Please refer to Documents 1, 3, and 4.

Some information within these documents has been withheld under the following sections of the OIA:

- 9(2)(b)(ii), as if released, it would be likely unreasonably to prejudice the commercial position of the person who supplied or who is the subject of the information.
- 9(2)(a), to protect the privacy of natural persons.
- 9(2)(g)(i), to protect the effective conduct of public affairs through the free and frank expression of opinions. Releasing the information would mean that the relevant staff will not be willing to convey their unguarded opinions in future, which is a core part of their role.

Where we have withheld information under section 9(2) of the OIA, we have considered any countervailing public interests in the release of this information. We do not believe that the public interests outweigh the need to withhold in this instance.

How to get in touch

If you have any questions, you can contact us at hnzOIA@tewhatuora.govt.nz.

If you are not happy with this response, you have the right to make a complaint to the Ombudsman. Information about how to do this is available at www.ombudsman.parliament.nz or by phoning 0800 802 602.

As this information may be of interest to other members of the public, Health NZ may proactively release a copy of this response on our website. All requester data, including your name and contact details, will be removed prior to release.

Nāku iti noa, nā

(PP)

Danielle Coe
Manager (OIAs) – Government Services
Health New Zealand | Te Whatu Ora

Appendix One

#	Title	Decision on release
1.	National Artificial Intelligence and Algorithm Expert Advisory Group – Meeting Minutes (Heidi Health agenda item) 25 October 2024	Some information withheld under sections: • 9(2)(b)(ii) • 9(2)(g)(i)
2.	AI Heidi Pilot Trial – Protocol Dated: 10 May 2025	Released in full.
3.	Ambient AI Scribes – What Good Looks Like Attachment: National AI & Algorithm Expert Advisory Group Review – Heidi Health: Ambient AI Scribe Assessment and endorsement	Released in full.
4.	Draft Terms of Reference	Released in full.
5.	Heidi Risks Overview	Released in full.
6.	AI Heidi Pilot Results	Some information withheld under section 9(2)(a) of the OIA.
7.	Heidi Summary Metrics (Omni Analytics Report) Generated: 12 January 2025	Released in full.
8.	Heidi Health Privacy Impact Assessment 27 June 2025	Released in full.
9.	Enterprise Services Agreement – AI Ambient Scribe (ESA) Data Processing Agreement (DPA)	Some information withheld under the following sections of the OIA: • 9(2)(b)(ii) • 9(2)(a)
10.	Data Processing Agreement – Heidi Health & Health New Zealand Signed: 10 October 2025	Released in full.
11.	Heidi Enterprise Implementation Overview	Released in full.
12.	Heidi AI Scribe AI Security Assessment Report 22 October 2025	Released in full.
13.	Enterprise Services Agreement – Heidi Health & Health New Zealand	Document withheld in full under section 9(2)(b)(ii) of the OIA.

Te Whatu Ora
Health New Zealand

National Artificial Intelligence and Algorithm Expert Advisory Group – Meeting Minutes

Date	25th October 2024
Location	Via Teams
Attendees	Robyn Whittaker (Chair), Jon Herries, Kevin Ross, Rochelle Style, Paul Muir, Greig Russell, Amanda Mark, Kerry Hiini, Rosie Dobson, Evo Leota-Tupou, Jamie Ioane, Cheng Kai (CK) Jin, Riki Kyle, James Oughton, Abtin Ijadi Maghsoodi, Matt Radford, Tan Xinxue, Lavan Mahes, Greig Russell, David McCormack, Matthew Strother
Apologies	Juliet Rumball-Smith, Matt Radford, Luca Ma, Darren Ritchie

Item	Details
	Karakia
3. (1110-1155)	Heidi Health: this agenda item is not seeking NAIAEAG endorsement but to gather the group's thoughts and concerns. Heidi has provided a NAIAEAG checklist, privacy impact assessment and data processing agreement. Presentation by team from Heidi Health • Background of Heidi Health provided. • Use around Australasia • Privacy policy explained – no data is used for AI training. Users are custodians of the data. • Once a session is deleted from Heidi, all data is removed from the system. • No difference in privacy policy between free and paid version Comments from the group • Concerns raised that this might be procurement of Heidi. Emphasised that the session is for Q+A. No procurement decisions will be made. • Comment raised that the information provided by the group can be highly valuable to the company and needs to be balanced with encouraging the company to make safe products. • Question raised over their privacy policy and data processing. Comment from Heidi that they are taking on board feedback from users and rework the privacy policy based on the feedback. Stated clear that no data is used for LLM model development. Data retention set out by the clinicians. Once a session is deleted from the system, all data is removed. State that they will only collect information to deliver the services of Heidi (e.g. email address). No difference in privacy policy between free and paid. Sharing of data with third parties only done to enable service delivery. • Question raised over how Heidi compares against its competitors. s9(2)(g)(i) • Question around the training process. Heidi health provides documentation/educational content on sign up. Provides live support. Education through use of the tool.

	• Question raised over how the product can be improved if no data is being used for training. Heidi reports that they have a number of ambassadors that provide feedback on the tool's development/road map. Also report that they have research collaborations with organisations where consent is gained from clinicians and patients around using data for product improvement. • Comment to the group to s9(2)(b)(ii) [redacted] • Question raised over data ownership. Report that Heidi does not claim to own any of the data and ownership lies with the patient. • Question raised over potential ways that Hiedi is mitigating automation bias and ways for QC. Heidi reports a large team of physicians whose role is to monitor Heidi's performance. Users can provide subjective feedback. Heidi can also track the number of times a user has edited the original note. • Question around the accuracy of the tool. Report that benchmark scores are not representative and different models can achieve different results on the same dataset. • Discussed legal implications of using Heidi – privacy laws, health information retention requirement, clear consent. Expressed concerns that privacy policy and provided documentation is not fit for NZ's context. • Question raised over the privacy policy and statements around data use for product improvement. Heidi states that this refers to the collation of clinician feedback to improve product. Reiterated that they don't use any health or sensitive patient information for any business improvement in anyway. Also used for analytic purposes but is not done for individual sessions. s9(2)(g)(i) [redacted] [redacted]

Background

Artificial Intelligence (AI) has an evolving list of applications, not least within medicine. Heidi is an ambient AI tool that can be used during a consult to 'listen', transcribe and summarise the consult into a desired output, e.g., clinic letter. There are several AI ambient software options available in New Zealand, none of which are in use by Health New Zealand. The rationale for piloting Heidi, relates to its cost, simple user interface and the fact that it is being readily used in both primary care and private secondary care clinics across Hawke's Bay.

Rationale for piloting ambient AI

Health targets has been a priority for the current Government, along with the expectation to deliver more volume. Many districts are operating at capacity, hence the need to explore options that could potentially increase clinician productivity that are cheaper than outsourcing to the private sector. Studies using a small volume of participants have been reported in the literature regarding the use of Heidi. The studies claim Heidi can reduce clinician admin time, cognitive burden and thus improve overall wellbeing of the clinician. To date there are no studies that test whether the reduction in admin time, correlates to an increase in productivity.

Primary Outcomes for pilot

1. Does Heidi improve productivity?
2. Does Heidi improve clinician wellbeing?

Ethics & Endorsements

- Ethics approval deemed unnecessary by central region committee as pilot more in line with a quality improvement project than research project.
- Endorsement for pilot to proceed across Hawkes Bay and Whanganui granted by the Deputy Chief Executive Central Region, Robyn Shearer.
- Acknowledgement of pilot granted by National AI governance group, with expectation that pilot outcomes reported back to group.
- Privacy impact assessment (PIA) for HNZ awaiting feedback on second draft.

Use of Heidi during pilot expectations

- Consent to be obtained verbally from all patients.
- Do not record patient NHI's in Heidi or during the consult.
- Ensure consults are deleted from Heidi after 7 days.
- Do not retain text transcripts of consults.
- All Heidi outputs must be reviewed and fact checked.

Outline of pilot

Heidi will be assessed in 2 phases, the first in ED and the second within the outpatient setting. A total of 40 clinicians will be used across Hawkes Bay and Whanganui. Clinicians eligible for the study include senior medical officers (SMO), resident medical officers (RMO) at registrar grade and above, nurse practitioners and specialist clinical nurses. The descriptors for each phase are as follows:

Phase 1: Emergency department setting

Clinician Eligibility: SMO/RMO & Nurse practitioners (max of 10 in each site)

Pilot duration: 2 months

Heidi potential uses:

- During a consult;
- Batch recording of consults with a view to completing clinical record after seeing multiple patients;
- Dictation of encounter after seeing patient – does not need to be as structured when recording a note as is often used to dictate a letter;
- Summary of discussion between colleagues;
- Capturing discussions during a resuscitation;

Capturing consultation data:

- Clinicians to provide Hendrix (Heidi franchise) with template designs for desired consult output in advance of pilot or during pilot as need evolves.
- Clinician uses either their phone or a microphone attached to a computer to record the encounter.
- Output from Heidi is transferred to clinical portal or relevant clinical application, after cutting & pasting the note.

Measuring outcomes:

1. Using business intelligence data, assess average number of consults seen per shift by each clinician 1 month prior to the pilot and then at Month 1 and Month 2 of the pilot.
2. Questionnaires relating to wellbeing (attached) to be completed before the pilot, at the end of Month 1 and end of the pilot.
3. Focus group to be arranged at end of the pilot that asks members the following:
    a. How would you rate the quality of your notes using Heidi?
    b. How have you used Heidi during the pilot?
    c. What feedback have you had from your patients?
    d. Has Heidi changed the way you interact with patients?
    e. Is Heidi a feasible solution for your environment?
    f. Have you identified any concerns with using Heidi?

End of Pilot:

- Clinicians undergoing the pilot may continue using the license for the remainder of the year, with the expectation the above outcomes will be reassessed as a part of a quality improvement process throughout this time.

Phase 2: Outpatient setting

Clinician Eligibility:

- SMO/RMO & Nurse practitioners/Clinical nurse specialists (max of 12 in each site)
- Clinicians must participate in outpatient clinical work

Date: 10/05/2025
Version: 2
Author: B Pearson, CMO

AI Heidi Pilot Trial - Protocol

Pilot duration: 3 months

Heidi potential uses:

- During a consult in outpatient or the acute setting.
- Dictation of encounter after seeing patient – does not need to be as structured when recording a note as is often used to dictate a letter;
- Dictation of non-contact appointments - does not need to be as structured when recording a note as is often used to dictate a letter;
- Summary of discussion between colleagues;
- Capturing discussions during a resuscitation;

Capturing consultation data:

- Clinicians to provide Hendrix (Heidi franchise) with template designs for desired consult output in advance of pilot or during pilot as need evolves.
- Clinician uses either their phone or a microphone attached to a computer to record the encounter.
- Output from Heidi is transferred to either clinical portal or dragon one (clinic letters), after cutting & pasting the note.

Pilot structure:

A standard clinic varies between specialities. Using medical specialties as an example, a standard clinic is 2 new patients and 5 follow ups. Over 3 months Heidi will be reviewed as follows:

Month 1 – clinician familiarises themselves with Heidi and how to use it. Clinician will do standard clinics.

Month 2 – clinician's standard clinic will increase with an additional follow up patient, e.g., 2 new patients and 6 follow ups.

Month 3 – clinician's standard clinic will increase with an additional new patient/first specialist appointment, e.g., 3 new patients and 5 follow ups.

Measuring outcomes:

1. Using business intelligence data, assess number of patients seen per clinic by each clinician 1 month prior to the pilot. Reassess clinic volumes at the ends of Month 1,2 and 3 of the pilot.
2. Questionnaires relating to wellbeing (attached) to be completed before the pilot, at the end of Month 1, 2 and 3.
3. Focus group to be arranged at end of the pilot that asks members the following:
    a. How would you rate the quality of your notes using Heidi?
    b. How have you used Heidi during the pilot?
    c. What feedback have you had from your patients?
    d. Has Heidi changed the way you interact with patients?
    e. Is Heidi a feasible solution for your environment?
    f. Have you identified any concerns with using Heidi?
    g. Is it feasible to increase your clinic capacity as a result of using Heidi?

End of Pilot:

Date: 10/05/2025
Version: 2
Author: B Pearson, CMO

- Clinicians undergoing the pilot may continue using the license for the remainder of the year, with the expectation the above outcomes will be reassessed as a part of a quality improvement process throughout this time.

Health New Zealand
Te Whatu Ora

Ambient AI Scribes – What Good Looks Like

Advancements in artificial intelligence (AI) are driving significant transformations in healthcare. Ambient AI scribes are a new category of AI technology that captures and summarises conversations between clinicians and patients into structured medical notes. These tools are increasingly being adopted across the healthcare sector, with multiple vendors offering similar solutions. Given this growing landscape, it is crucial to establish clear expectations for their deployment within Te Whatu Ora – Health New Zealand (Health NZ). This document sets out Health New Zealand's requirements for AI scribe vendors and provides implementation and evaluation details for Health NZ staff.

Understanding the Technology

Understanding the technology behind AI scribes is critical to ensuring their safe and effective use within Health NZ. To better understand the technology, three key areas are considered; data, model and the monitoring process.

Data

Health NZ requires a clear understanding of the data processed by the AI scribe, including how and where Health NZ data will be processed and the plans for its secure disposal.

Transparency in the development process is essential, as it provides insight into how the tool has been built, the development process for future functionalities, and highlights any potential limitations arising from its design. Without a well-defined and structured approach to introducing new features, patient privacy and clinical safety may be compromised.

The training data used to develop the AI scribe must be diverse and relevant to the intended healthcare application. Overseas-developed commercial products will likely require localisation to fit the New Zealand healthcare context. Health NZ will need to understand how the localisation will occur, including whether the process will require data sourced from Health NZ's consumers and what measures will be in place to ensure ethical and secure data use. Furthermore, Health NZ will need clarity on whether consumer data will be used for ongoing AI development or to improve the AI tool.

The processing of clinical conversations constitutes personal information and is subject to the New Zealand Privacy Act. The Act allows processing of personal information in jurisdictions with privacy regulations comparable to those of New Zealand. Therefore, Health NZ must have a clear understanding of where this information is processed, including any third parties or sub processors involved in data handling on behalf of the vendor.

Model Architecture

AI scribes generally operate in two key steps: first, a conversation is converted into a transcript, and a large language model processes the transcript to generate a clinical document. Health NZ requires an understanding of both steps to identify potential limitations, develop mitigation strategies, and collaborate with vendors to address any concerns.

There are numerous models available for voice-to-text transcription, but these are typically developed by international companies and often have limited capability in recognising Te Reo Māori and other languages spoken by minority communities in New Zealand. Therefore, Health NZ requires a clear understanding of the steps vendors are taking to localise their product to the New Zealand context.

Once a transcription of a conversation is generated, a large language model is prompted to generate a clinical documentation. The exact structure of the clinical documentation is dictated by the prompt used and curated examples. This process presents several risks which Health NZ seeks clarification on:

1) Large language models are known to have inherent bias and can 'confabulate'. We seek evidence that these areas have been evaluated, and steps taken to mitigate these factors.
2) Health NZ is a large organisation with different ways of documentation across the organisation. We need to understand the vendor's level of control over developing new prompts to suit Health NZ's requirements and whether data from Health NZ is required in the process to fine-tune or improve the tool.
3) Health NZ anticipates that vendors will regularly update their AI scribe products to enhance performance and introduce new functionalities. Although continuous improvement is desirable for Health NZ, these updates will introduce potential risks. Health NZ requires clarity on the update process including the testing process conducted before deployment and the parties responsible for monitoring performance post-update to ensure safety, reliability.

AI scribes are new tools for Health NZ and are taking a cautious approach to their use and implementation within the organisation. Understanding the model's provenance is essential for assessing its reliability, safety, and suitability for clinical use. Transparency in these areas will help Health NZ to effectively evaluate the product and support its safe implementation.

Monitoring

Ensuring the accuracy of AI generated outputs is one of Health NZ's primary concerns with AI scribe tools. Errors in medical documentation can lead to clinical mistakes, compromise patient safety, and result in serious harm. Given these risks, Health NZ seeks understanding on the process taken to ensure accuracy, relevance, and consistency of the generated content from the AI tool.

This will require understanding of both pre-release testing and a monitoring process as part of routine use. The monitoring process should include system-level reporting, such as tracking the extent of clinician modifications to AI-generated content, as well as a structured mechanism for feedback and continuous improvement, such as flagging incorrect summaries. In cases where inaccurate summaries are generated, vendors must have a clear policy for managing these discrepancies, including an established process for investigating root causes, and implementing improvements. Health NZ expects vendors to demonstrate how they will use clinician feedback to refine model performance and prevent recurring errors.

Impact on Patient and Clinical Workforce

Clinical Workforce Impact

AI scribes represent a significant shift in clinical documentation, changing the way medical notes are generated and requiring adjustments to existing workflows. With AI scribes, clinicians' internal reasoning, observations, and decision-making processes will need to be verbalised for the tool to capture and structure information appropriately. This change may require clinicians to adjust their consultation style, ensuring that key clinical details are spoken aloud rather than assumed as implicit knowledge. Vendors must support this transition through education and training programmes that help clinicians adapt their communication. The training will need to include best practices for verbalising key clinical details, strategies for structuring consultations to ensure accurate AI-generated notes and understanding potential limitations of AI-generated documentation. A structured onboarding process will be essential to ensure clinicians feel confident in using AI scribes effectively while maintaining high standards of documentation accuracy and completeness.

The role of clinicians in reviewing and validating AI-generated documentation is critical to ensuring accuracy, safety, and reliability. Clinicians ultimately remain responsible for their notes, and AI-generated outputs must not bypass their clinical oversight. Clinicians will need to have the ability to review AI-generated content immediately before it is finalised in the patient record. The system will need to allow for easy editing, correction, and refinement of notes to ensure clinical accuracy. There should be a clear audit trial between AI-generated content and clinician modifications. Without proper oversight, there is a risk that inaccurate or incomplete notes could enter the patient record, leading to potential clinical errors.

Lastly, clinicians must have the ability to enable or disable AI assistance at their discretion. There will be scenarios where the use of an AI scribe may not be appropriate, such as highly sensitive conversations or cases where a clinician prefers traditional note-taking methods. Vendors should provide clear guidelines on how and when clinicians can toggle AI scribes on or off.

Patient Perspectives

Patient consent is required before an AI scribe can be used in a clinical setting, ensuring transparency and maintaining trust between healthcare providers and patients. The consent process must be clear, comprehensive, and structured, allowing patients to make informed decisions about the use of AI scribes in their care. Health NZ will require a clear understanding of the consent process to effectively communicate with our patients. The consent process will need to address the following areas:

1) How patient data will be used, including whether it will contribute to the improvement of the vendor’s products or the further development of the AI tool.
2) The involvement of any third-party vendors or partners in enabling or supporting the AI scribe.
3) Clear details on who will have access to stored data, including whether it can be accessed for secondary use.

In situations when patients choose to opt out of AI scribe use, there must be a clear and established process to ensure their preference is respected without disrupting their care.

Evaluation

The evaluation of AI scribe tools will determine whether these emerging technologies can reduce the administrative workload of clinicians at Health NZ. This assessment will integrate both vendor-supplied performance data and direct feedback from clinical users. The goal is to evaluate the benefits of AI-powered scribing solutions while ensuring high standards of clinical accuracy and quality of care are maintained.

System measures:

Although specific data requirements may vary depending on each vendor's technical capabilities and data collection methods, the following metrics are recommended:

1. Usage analytics by user (and service where appropriate) [**obtained from vendor**]
    a. Number of sessions/encounters processed: Total count of documented clinical interactions using the AI tool.
    b. Session completion vs. abandonment rates: Ratio of fully completed sessions to those started but not finalised.
    c. Duration of recording sessions: Average length of each AI-assisted documentation session.
    d. User login frequency and session patterns: Frequency of clinician interactions with the tool.
    e. Feature utilisation rates: How often specific functionalities (e.g. referral drafting) are used.
2. Documentation quality metrics **[obtained from vendor if available]**
    a. Post-generation edits by user**:** Number and type of changes user makes to AI-generated documentation.
    b. Correction categories: Classification of edits into key areas (e.g. medical terminology, clinical accuracy, formatting, content structure).
3. Service Impacts **[obtained from service]**
    a. Impact on the transcription service (i.e. changes in document turnaround times)
    b. Impact on clinical efficiency (i.e. number of patients seen in clinic/ED).

User measures

As part of the evaluation process, Health NZ will also conduct user (clinician) surveys to capture direct user experiences with AI scribe tools. This feedback will be required to understand user satisfaction, perceived efficiency, ease of use, and the overall clinical value of these technologies. To ensure robust data collection, surveys will be administered at multiple timepoints throughout the evaluation period (e.g., baseline, 1 month and 3 months), allowing assessment of both initial impressions and sustained benefits as clinicians develop proficiency and confidence with the technology. The survey will be anonymous but individual surveys linked through REDCap to allow for changes to be assessed. The survey will aim to evaluate the following areas:

1. Perceived benefits including reduction in time spent on clinical documentation: Clinician perceptions of whether the AI tool has meaningfully decreased the time required for clinical documentation.
2. Improvement in completeness and accuracy of clinical notes: Clinician perceptions of enhancements in clarity, completeness, or overall quality of clinical notes produced with AI support.

3. Improvement of clinician-patient interactions during consultations: Whether the use of the AI scribe has enabled more face-to-face time, improved communication, or enhanced patient engagement.
4. Frequency and type of errors, significant omissions or confabulations in the outputs: Incidence of significant inaccuracies, missing information, or fabricated content in the AI-generated outputs.
5. Concerns regarding the use of AI Scribes: Any issues clinicians have regarding using AI-assisted documentation.
6. Time required to achieve proficiency with the tool: The amount of time and support required for clinicians to become comfortable and proficient with the tool.
7. Recommendations for ongoing use and sustainability.

The survey will be distributed via REDCap and made available to all participating evaluation sites. Analysis will be performed by the AI Lab Research and Evaluation team and results provided by service where appropriate.

Māori and Equity Considerations

From a Māori and equity perspective, AI scribes must be adapted to the New Zealand context, ensuring they can accurately detect and understand commonly spoken languages, including te reo Māori, as well as other languages prevalent within New Zealand's diverse communities. This adaptation is essential to provide equitable healthcare and ensure that AI technology is accessible, inclusive, and culturally sensitive for all populations. Furthermore, the tool must be developed to avoid biases that may affect Māori or other minority communities, ensuring fair and unbiased documentation.

Legal Considerations

The AI scribe tool must comply with New Zealand's privacy laws, which governs the collection, storage, and use of personal data. Compliance with these laws ensures that patient data is handled according to local legal standards, providing necessary protections for patient privacy. Additionally, a data processing agreement (DPA) should be established to clearly outline how patient data will be utilised by the vendor. This agreement must specify the processes for data collection, storage, access, and security, as well as how or if the data will be used to improve the AI tool. It should also define the roles and responsibilities of all parties involved, ensuring transparency and accountability in the management of sensitive healthcare data.

Standards for AI Scribe Use in Health NZ

These standards define the minimum requirements for the safe, effective, and ethical use of ambient AI-based clinical scribe technology within Health New Zealand (Health NZ).

General Considerations

- **Localisation and Language Inclusion**: AI scribes must be developed or include plans to accommodate New Zealand's diverse spoken languages, including support for Te Reo Māori and other minority languages. In addition, local clinical terminology and consultation styles must also be reflected.
- **Continuous Monitoring and Improvement**: Vendors must maintain and provide a documented plan for the ongoing monitoring, maintenance, and improvement of AI scribe tools.
- **Informed Consent**: A clear, transparent, and structured consent process must be developed by vendors, allowing patients to make informed decisions about the use of AI scribes in their care. The consent procedures must explain how the technology works, what data is collected, how it will be used or retained and deleted.
- **Bias Mitigation and Testing**: AI tools must be designed and tested to actively avoid bias in documentation, particularly against Māori and other minority populations.
- **New Zealand Company Registration**: Vendors providing AI scribe solutions must be registered to operate in New Zealand. This ensures legal accountability, and alignment with local regulatory and privacy frameworks.

Privacy and Data Governance

- **Regulatory Compliance**: All data handling must comply with the Privacy Act 2020 and the Health Information Privacy Code 2020.
- **Data Processing Agreements**: A Data Processing Agreement (DPA) must be established. Vendors will need to agree to the following terms:
    - Clear limitations on data use, ensuring data is solely used for clinical note generation.
    - Explicit prohibitions, unless agreed to by Health NZ, on the use of patient data for AI training, commercialisation or product improvement.
    - Inclusion of vendor security obligations and audit rights for Health NZ.
    - Strong protections against unauthorised data sharing.
    - Clear provisions requiring data to be stored and processed within New Zealand or Australia.
- **Data Minimisation and Retention**: Only the minimum necessary data should be collected and in accordance with NZ legislation. Retention and deletion policies must be clearly defined, enforceable, and auditable.

Clinical Safety and Performance

- **Functionality and Versatility**: AI scribes must be capable of generating high-quality clinical notes across a wide range of specialties, clinical contexts, and consultation types.
- **Clinician Training and Support**: Vendors must provide onboarding and training for clinicians. This should include:
    - Best practices for verbalising key clinical details.
    - Understanding the limitations and ways of appropriate use.
- **Audit and Quality Assurance**: Vendors must support ongoing auditing processes to assess quality, privacy compliance, and alignment with Health NZ's expectations for data stewardship.

Security

- **Role-Based Access Controls**: Systems must include granular role-based access controls to ensure only authorised users can view or edit sensitive clinical information.
- **Security Standards Compliance**: Vendors must demonstrate compliance with internationally recognised security frameworks SOC 2 (System and Organisation Controls 2) or ISO/IEC 27001
- **Alignment with Government Cybersecurity Standards**: Systems must meet or exceed the New Zealand Government's cybersecurity assessment and assurance requirements, including vulnerability testing, incident response planning, and regular system audits.
- **Encryption Standards**: All data in transit and at rest must be encrypted using current best practices.

Health New Zealand
Te Whatu Ora

National AI & Algorithm Expert Advisory Group Review

Requesting Service:	**Heidi Health,** Lara Hopley
Assessment Date:	30th June 2025
Subject:	**Heidi Health – Ambient AI Scribe**

Heidi Health is an ambient AI scribe vendor seeking endorsement from the National AI and Algorithm Expert Advisory Group (NAIAEAG) for use within Health New Zealand – Te Whatu Ora (Health NZ). The product leverages advanced voice recognition and large language models to transcribe clinical conversations between patients and clinicians into structured clinical letters or documentation.

NAIAEAG initially reviewed Heidi Health in October 2024 and raised concerns relating to patient privacy and data governance. In response, a Privacy Impact Assessment and a Cloud Risk Assessment were completed, both of which advised that formal contractual agreements are required to ensure appropriate safeguards for patient privacy and data protection. The following key considerations must be addressed during future pilots and implementation phases, and specifically applies to the enterprise/paid version of Heidi Health:

1) Workflow considerations: Heidi Health is not currently integrated with Health NZ's electronic systems, and workflows may vary across regions and services. Adoption of this tool will have implications for existing transcription processes. Services must engage with local transcription teams to ensure integration into current workflows and compliance with Health NZ documentation standards.
2) Procurement and Contractual: A Master Service Agreement must be established with Heidi Health to ensure legal protections are in place for patient data. Use of the free version of the tool is not permitted, as it does not meet Health NZ's privacy, security, or contractual standards.

Health NZ supports the adoption of innovative solutions that can reduce administrative burden and improve the timeliness of clinical documentation. Based on the assessments undertaken and subject to the above considerations, NAIAEAG endorses further piloting and evaluation of the Heidi Health solution within Health NZ.

Ngā mihi

Dr Cheng Kai (CK) Jin (he/him)
Clinical Director | Artificial Intelligence Laboratory
Planning, Funding and Outcomes

Proposal for the Development, Validation, or Implementation of a new AI

Principal Investigator/Lead	
Clinical Lead	
Project Name	
Date Submitted	

Purpose

Describe the problem the AI is trying to solve, the scale of the problem, inequities, how many people it impacts, the impact for Māori, and current solutions/management. Why is AI appropriate in addressing this problem? What are the anticipated benefits and risks of using the AI.

Problem AI is trying to solve, the scale of the problem, inequities, how many people it impacts, the impact for Māori

Clinicians in New Zealand are at high risk of burnout, and clinical administration is a large contributing factor to this. The amount of mental burden clinicians need to carry from all the consults they do in all settings, to then recall that information into high quality summary notes and letters is something that is a major problem which clinicians not only in New Zealand face [1], but also across the globe. The problem is exacerbated within hospital settings, especially emergency departments (where patient care is urgent).

Heidi Health is an AI ambient scribe product aimed to reduce this mental and clinical administration burden. Heidi Scribe can be turned on during a consultation between a doctor and a patient, it listens to the full conversation and the transcript is used to develop notes, letters and documents at a click of a button. Heidi is inherently a configurable product, whereby a custom note or document template can be created and stored for future use, to generate the same documents in the same structure, for every consult. In addition, having Heidi Scribe listening in the background means a doctor can trust that the service will be taking notes, and the doctors can go back to practicing medicine and developing deep relationships with their patients - impacting the whole NZ population including *Māori* to receive better clinical care and have a better clinical experience.

The usage of an ambient AI scribe not only saves clinician time, but in fast paced settings like emergency departments where clinical time is crucial, there is a significant impact on improving patient flow and ensuring patients are being treated within target time frames.

Current solutions/management, and why is AI appropriate to address this problem

There are very few current solutions without the use of AI which would have the same impact a product like Heidi Health could make on a clinician's time. The non-AI solution for this issue would be to hire a Medical Scribe or establish a typist team, where doctors would still have to use dictation software to dictate their notes and have the typist teams digest and summarise it. Heidi's product has shown that AI has evolved to a point where it can help in not only support in the capturing of clinical information, but high quality summarisation and document generation can now be done efficiently and at speed. For reference, a typical average typist would type at 80 words per minute, not including reading and comprehension time. Heidi can develop a summary at a speed of 600 words in 6 seconds.

Anticipated benefits and risks of using the AI

DRAFT **Terms of Reference**
AI Operational Leadership Group

Purpose
The AI Operational Leadership Group provides leadership, prioritisation, and oversight for operational implementation of AI initiatives endorsed by the National AI and Algorithm Expert Advisory Group (NAIEAG). The group ensures AI adoption aligns with organisational strategy, government priorities, and best practice, while maintaining clear visibility of AI activity across Health New Zealand.

It acts as an advisory body to the Executive Leadership Team (ELT) on AI operational matters and outcomes. The group's focus is on operational leadership and system-wide coordination, not project delivery governance.

Scope
The group's remit includes:

- Prioritising (or de-prioritising) implementation of AI initiatives endorsed by NAIAEAG based on factors such as fit with organisational priorities and feasibility of/readiness for adoption.
- Facilitating implementation, directing resources, and addressing unnecessary blockers to implementation of prioritised projects.
- Monitoring outcomes and value realisation from implemented AI use cases, including benefits, risks, and lessons learned.?
- Working with NAIAEAG on operational, policy, and strategic responses to emerging AI technologies and government directives.
- Reporting to ELT as necessary, on AI related matters, such as emerging technologies and issues.
- Considering both clinical and non-clinical AI tools, although with the ability to have different 'speeds' or pathways for different levels of risk, with clinical AI tools being generally higher risk

---

Membership

- Core membership comprises:
    - Senior Digital Lead: Sonny Taite
    - Senior Clinical Lead: Helen Stokes-Lampard
    - People & Culture Lead: Fiona McCarthy (or delegate)
    - Planning, Funding and Outcomes/ELT Lead: Jason Power
    - Data: Stuart Bloomfield

- Other members include:
    - Digital Services: Lara Hopley, Ed Falloon, Sarndrah Horsfall, Jon Herries
    - NAIAEAG: Robyn Whittaker (chair), CK Jin (AI Lab)
    - Procurement:
    - As needed: communications, legal, privacy, clinical safety, and workforce as required.
- Members must have sufficient authority to inform cross-portfolio prioritisation and operational alignment.
- Delegation is encouraged when primary members are unavailable to maintain continuity.

Ways of Working

- Meet regularly, with frequency determined by the pace of AI developments and operational needs, with the ability to convene for urgent matters.
- Proactively identify and prioritise areas for AI adoption based on system needs and opportunities; as well as respond to proposals coming through from NAIAEAG and the Health Technology Evaluation Pathway (appendix)
- Ensure clear communication pathways internally and externally, ensuring consistent messaging about AI adoption, risks, and benefits.
- Ensure that the group has appropriate links to relevant cross-governmental AI leadership and groups (e.g. DIA, GCDO, MoH, PHOs)
- AI Lab (Robyn Whittaker, CK Jin & Jon Herries) will maintain a list/flow of topics to come through the group.

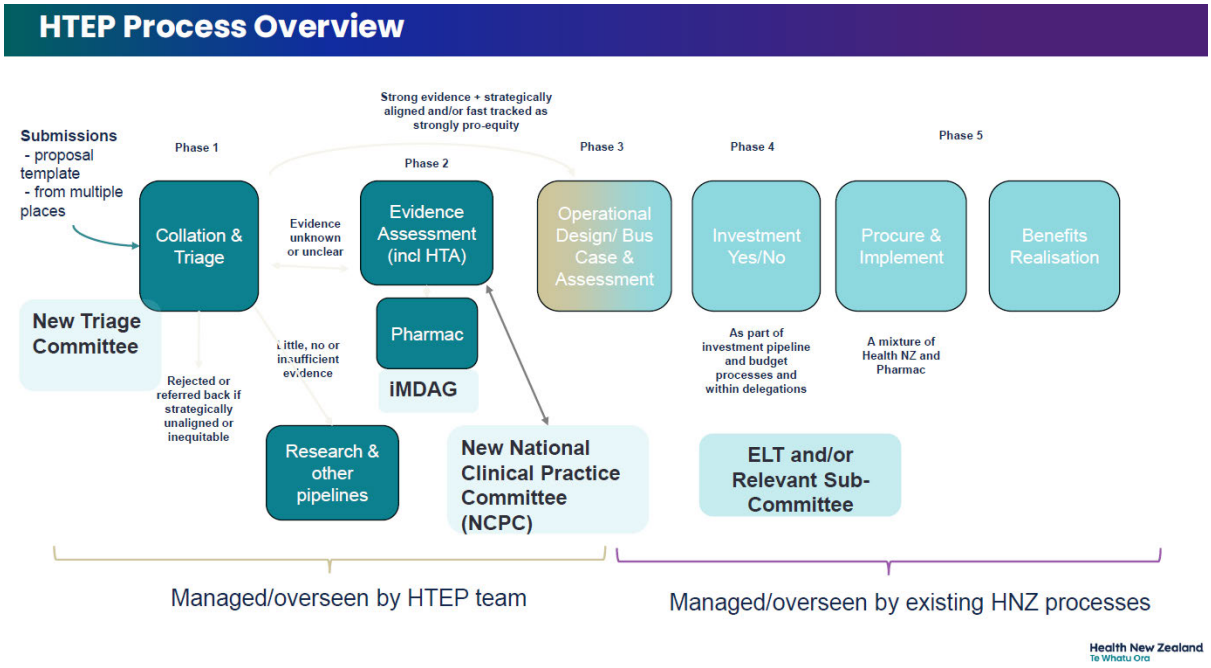
Reporting

- Report directly to the ELT, providing updates on operational AI priorities, progress, benefits realisation, and issues requiring executive attention.
- Ensure reporting is integrated with broader governance, investment, and performance processes.

Review of Terms of Reference
These Terms of Reference will be reviewed annually or sooner if significant changes occur in the AI landscape or organisational context.

Appendix: Health Technology Evaluation Pathway – to discuss how or whether we fit in with this existing front door and pathway – James le Fevre happy to come to a meeting to discuss

HTEP = *a single nationally-consolidated, systematic process for triaging, assessing, and appraising health technologies to inform their adoption and use within the New Zealand public health system*.



Executive Summary: Heidi AI Risk Themes and Mitigations

This summary provides a consolidated view of the key risk themes, issues raised, and mitigation approaches identified across emails, Teams discussions, and working-group materials relating to the rollout of Heidi AI in clinical settings.

1. Privacy, Consent, and Assurance

The programme is operating under a transcript-only retention model, with no audio recording by default. Questions have been raised about whether enabling audio would alter the privacy posture and require a refreshed Privacy Impact Assessment and updated clinician/patient communications. Additional guidance is being developed for under-16 consent scenarios, following feedback from clinical teams. Public commentary on digital health tools has increased sensitivity to privacy and security messaging.

2. Identity, Access, and Technical Onboarding

SSO is not yet enabled, resulting in reliance on emailed access codes that can be delayed. Several districts require additional time to complete network allow-listing, creating variability in onboarding timelines. Interim workarounds and clearer user guidance have been implemented, with SSO planned for a future update.

3. Clinical Safety and Documentation Quality

Clinical teams have highlighted risks related to AI hallucinations, template completeness, and the need for consistent process controls (e.g., auto-logout, disclaimers). Documentation for the mental state examination (MSE) has been updated to ensure completeness, with positive early feedback. Metrics to track safety-related behaviours (e.g., disclaimer use) are being incorporated into operational dashboards.

4. Data Sovereignty, Cost, and Vendor Dependence

Public discussions have focused on data sovereignty and the long-term cost profile of commercial AI scribes. To reduce vendor lock-in and maintain flexibility, a panel procurement approach and transparent value tracking are being explored.

5. Workflow, Integration, and Environmental Factors

Compared with T Pro, Heidi currently requires a manual step to attach notes to Clinical Portal, introducing workflow friction. Environmental challenges particularly noise levels and device reliability in Emergency Departments affect transcription quality. Updated guidance on noise mitigation, hardware, and telehealth workflows is being integrated into onboarding.

6. Governance, Onboarding Model, and Workforce Engagement

Onboarding has sometimes been site-led rather than centrally coordinated, creating variability in training and oversight. The AI Operational Leadership Group is developing a consistent operating model covering communications, training materials, and governance structures. Union engagement and broader change-management activities are ongoing to support workforce confidence and acceptance.

7. Communications, Media, and Public Messaging

A high frequency of media queries has increased the need for coordinated, consistent messaging. Approved lines emphasising evidence, governance, and scope are being reused to ensure accuracy and alignment across channels.

8. Role Design, Permissions, and Analytics

Feedback indicates a need for more granular user roles, as the current admin licence grants broad access while assistant roles lack essential functions. Separately, enhanced usage analytics and safety monitoring capability is under development to improve visibility of adoption, template usage, and risk controls

Title:
Evaluating the impact of an Artificial Intelligence ambient scribe on productivity and clinician wellbeing in the Emergency Department: a pilot study

Short title:
AI Scribe: ED efficiency and wellbeing

Key Words:
Artificial Intelligence, Scribe, Emergency Department, Emergency Medicine

Authors:

Dr Charles Gregory MBBCh (Hons)
Emergency Department Registrar
Te Whatu Ora Hawke's Bay
s9(2)(a)

Dr Simon Harger
Emergency Department FACEM and Head of Department
Te Whatu Ora Hawke's Bay
s9(2)(a)

Dr Benjamin Pearson
Paediatric Consultant and Chief Medical Officer
Te Whatu Ora Hawke's Bay
s9(2)(a)

Ethics

Approval for this pilot has been given by Te Whatu Ora following an assessment of privacy risks. Hendrix Health has provided privacy safety information for the project. Patient consent was required for each consultation where Heidi was used. Information about the pilot and the use of Heidi is being communicated to patients via posters in the department and direct communication by clinicians as needed.

Evaluating the impact of an Artificial Intelligence ambient scribe on productivity and clinician wellbeing in the Emergency Department: a pilot study

Abstract:

Objective:
This proof-of-concept pilot evaluated if Heidi, an Artificial Intelligence (AI) software increased productivity and wellbeing of clinicians working in an Emergency Department (ED).
Methods:
The mean number of patients seen per shift by 10 clinicians over an 8 week period pre and post implementation. Qualitative data was collected over the same period through surveys to investigate clinicians confidence in the AI tool and wellbeing.
Results:
The mean number of patients seen by clinicians per shift increased by 0.9 with AI and clinicians subjectively reported spending significantly less time documenting notes. Feelings of burnout reduced by 26%.
Conclusion:
Using AI within the ED increased productivity and reduced burnout. Further research on larger sample sizes over longer periods are needed to see if these benefits are generalisable.

Key words:
Artificial Intelligence, Scribe, Emergency Department, Emergency Medicine

Objective

Artificial Intelligence (AI) in healthcare is a rapidly evolving field that utilises software to undertake tasks commonly associated with clinical care.

Documentation burden is a significant contributor to clinician workload, burnout and reduced patient safety in Emergency Medicine (1, 2). Previous studies have suggested that the use of Artificial Intelligence (AI) driven tools may be effective in alleviating some of this burden. This includes studies from some small private centres in New Zealand, however this has not, to our knowledge, been trialled in the public sector (3, 4) .

This proof-of-concept pilot study aims to evaluate whether the use of an ambient AI scribe, improves the efficiency and wellbeing of clinicians working within the Emergency Department (ED) at Te Whatu Ora Hawke's Bay, New Zealand. Heidi is an ambient AI medical scribe that aims to automate clinical documentation by transcribing clinical interactions. It uses a specifically trained Large Language model (LLM) to reformat the transcription into a coherent and structured clinical document. This tool has the potential to reduce the time spent on documentation, increase the number of patients seen and reduce the cognitive burden and work load of clinicians.

Methods

This pilot study involved ten ED clinicians (four Senior Medical Officers (SMO), four Registrars and two Nurse Practitioners). Data were reviewed for two eight-week periods before and after the implementation of the AI tool. A combination of qualitative and quantitative metrics were used to assess effectiveness. In the eight weeks before implementation the mean number of patients seen per shift by each clinician was counted and a questionnaire completed looking at the clinician's perceived documentation burden, well-being and satisfaction in the AI tool. This process was repeated over a second eight-week period post implementation. For transcription, clinicians used the Heidi app on their mobile phones. Patients were prospectively verbally consented with the app providing a prompt for this process. The app then recorded the consultation and subsequently

created a patient note. Generated documents were copied and pasted into the hospital's electronic medical record via the Heidi website.

Results

During the pilot period, the mean number of patients seen per shift by clinicians increased by 0.9 (+3.9 to -2.6). There was interpersonal variability between clinicians, including two clinicians who saw fewer patients per shift during the pilot when compared to before. In one case this was related to a clinician transitioning from a registrar to an SMO.

The subjective data from the survey responses indicate that the time spent on documentation per patient was reduced by an average of 64%, from 16 to 6 minutes, while the time documenting outside of work hours was reduced by 81%, from 10.5 to 2 minutes. Clinicians also reported a perceived increase in note comprehensiveness and the manageability of documentation, which they associated with reduced feelings of burnout and increased confidence. Survey comments indicated that even with occasional transcription inaccuracies, the established process of manual review and editing by clinicians ensured accuracy prior to publication, thereby maintaining the tool's overall positive effect on workflow.

Conclusion

Within this pilot, the use of an ambient AI scribe was found to increase the mean number of patients seen by clinicians per shift, while also reducing feelings of stress and burnout. Clinician confidence in the system grew with use, and importantly, levels of patient acceptance appear high.

Following the results of this pilot, we intend to expand the pilot within Emergency Department clinicians and to other groups within the hospital. While currently in its early phases, we believe this tool shows promise as a way to both increase clinician productivity and decrease cognitive load.

As global demands on Emergency Departments continue to grow, this study highlights the exciting possibilities in using AI to aid patient care and free up clinician time. Further research across multiple settings will help to expand our understanding of how AI tools can support healthcare.

References

1. Gardner RL, Cooper E, Haskell J, Harris DA, Poplau S, Kroth PJ, et al. Physician stress and burnout: the impact of health information technology. Journal of the American Medical Informatics Association. 2018;26(2):106-14.
2. Hall LH, Johnson J, Watt I, Tsipa A, O'Connor DB. Healthcare Staff Wellbeing, Burnout, and Patient Safety: A Systematic Review. PLOS ONE. 2016;11(7):e0159015.
3. Gandhi TK, Classen D, Sinsky CA, Rhew DC, Vande Garde N, Roberts A, et al. How can artificial intelligence decrease cognitive and work burden for front line practitioners? JAMIA Open. 2023;6(3):ooad079.
4. Ballantyne A, Style R, Stubbe M, Murton S, Dowell T. Using AI scribes in New Zealand primary care consultations: an exploratory survey. Journal of Primary Health Care. 2025.

Figures/Tables

Table 1 – Qualitative clinical feedback survey

Questions	Pre	Post	% Difference
On average, how many minutes do you currently spend documenting notes per patient encounter?	16.20	5.90	64%
On average, how many minutes per day do you spend completing clinical documentation outside your rostered hours?	10.50	2.00	81%
Clinical documentation currently consumes a manageable portion of my ED shift workload (score out of 10)	5.80	9.30	60%
Overall, how satisfied are you that your current clinical documentation process results in a comprehensive picture of your patient interaction? (score out of 10)	5.10	8.20	61%
How confident are you that documentation generated using Heidi clearly reflects your clinical decisions and patient interactions? (score out of 10)	6.10	8.30	36%
To what extent does your current documentation workload contribute to feelings of stress or burnout? (score out of 10)	4.20	3.10	26%
To what extent do you expect Heidi will improve the overall quality of your clinical documentation? (score out of 10)	6.40	6.90	8%
How confident do you currently feel about using an AI-powered documentation tool like Heidi regularly during patient encounters? (score out of 10)	5.30	9.40	77%

Table 2 – Qualitive review of number of patient seen per shift

Clinician	Patients per Shift Pre-Pilot	Patients per Shift During Pilot	Change per shift
ED Registrar	5.3	8.8	3.5
ED Registrar	6.5	7.8	1.3
ED Registrar	4.7	8.5	3.8
ED Registrar	7.9	8.0	0.1
ED Registrar/SMO	6.0	2.9	-3.1
ED SMO	3.3	3.3	0.0
ED SMO	4.8	5.0	0.2
ED SMO	3.7	4.7	1.0
ED Nurse Practitioner	8.5	11.9	3.4
ED Nurse Practitioner	12.1	11.0	-1.1
Average gain in patients seen per shift/clinician			0.9

Footnote:
Clinician labelled ED Registrar/SMO transition from Registrar to SMO halfway through the pilot study

Health NZ

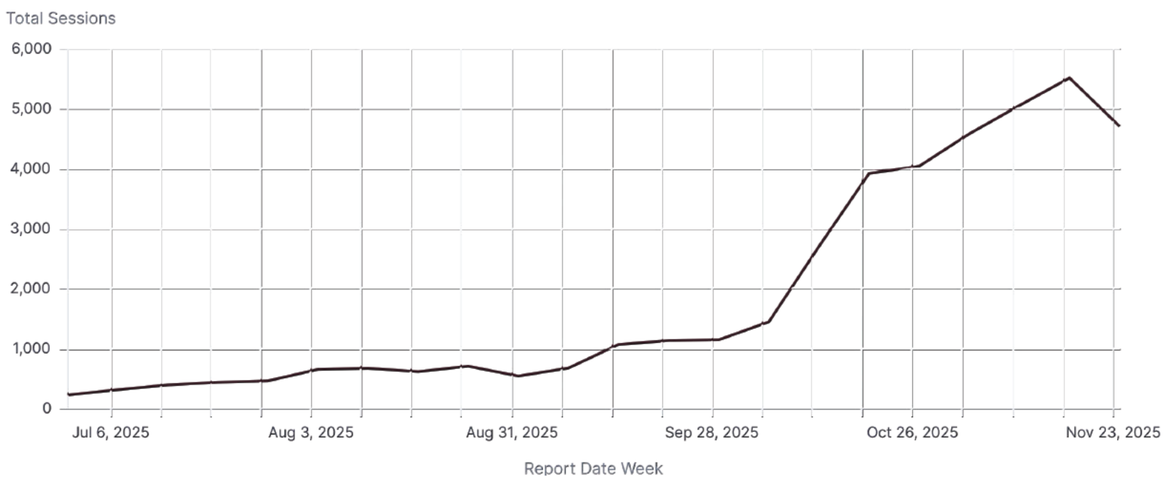
Overview

	Team Name	ED User count	User Count	Users With Session	Activation Rate	Event Minutes Dictated Sum	Event Minutes Transcribed Su	Ask AI Document Cou
1	Health NZ - Central - MH	0	118	30	25.42%	71.45	4,291.82	6
2	Health NZ - Counties - Hospc Sv	0	2	0	0%	0.32	0.32	0
3	Health NZ - Dunedin - ED	11	21	13	61.9%	71.57	600.07	0
4	Health NZ - Dunstan Hosp - ED	1	4	2	50%	0	345.9	0
5	Health NZ - Invercargill - ED	3	8	3	37.5%	4.7	35.07	0
6	Health NZ - Lakes - MH	0	16	8	50%	118.35	1,216.75	0
7	Health NZ - Rotorua - ED	10	49	24	48.98%	26.15	3,043.1	4
8	Health NZ - Taupo - ED	4	13	8	61.54%	155.3	5,305.48	0
9	Health NZ - Waikato - ED	4	73	3	4.11%	0.03	618.33	0
10	Health NZ - Wairarapa - Hospc Sv	0	6	3	50%	18.1	13,517.65	48
11	Health NZ - Wairau - ED	2	8	1	12.5%	10.53	10.53	0
12	Health NZ - Whangarei - AH	0	1	1	100%	0	8.53	0
13	Health NZ – Auckland – Hospc Sv	32	56	46	82.14%	716.32	20,294.92	42
14	Health NZ – Canterbury – ED	83	115	84	73.04%	1,051.18	43,908.33	0
15	Health NZ – Canterbury – Hosp Svs	0	99	87	87.88%	3,234.6	77,121.48	192
16	Health NZ – Counties – ED	70	106	97	91.51%	3,306.38	84,287.53	98
17	Health NZ – Counties Manukau – MI	0	29	22	75.86%	740.63	24,280.13	12
18	Health NZ – Hawke's Bay – ED	48	82	68	82.93%	1,420.3	120,941.75	8
19	Health NZ – Hawke's Bay – Hosp S.	5	44	37	84.09%	5,317.83	79,714.17	20
20	Health NZ – Nelson Marl – ED	24	37	30	81.08%	63.93	11,513.5	0
21	Health NZ – Tairāwhiti – Hospc Sv	4	62	41	66.13%	446.77	16,745.5	4
22	Health NZ – Taranaki – Hospc Sv	26	78	47	60.26%	234.48	19,823.52	12
23	Health NZ – Tauranga – Hospc Sv	18	30	19	63.33%	1,175.65	8,107.32	2
	Total	451	1,273	797	62.61%	20,019.63	613,643.47	566

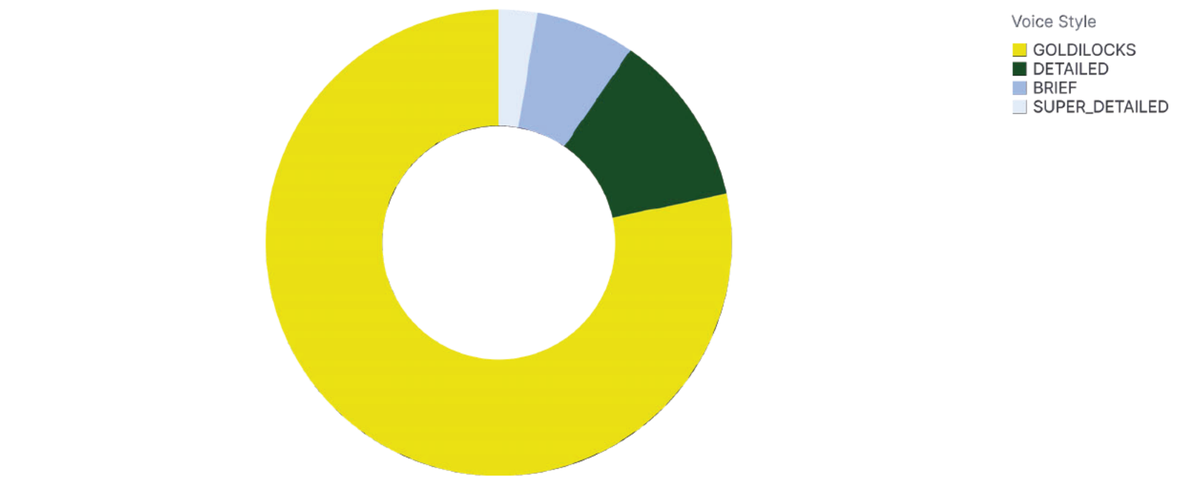
Template Usage

	Template Nam	Team Nam	Consult Not Coun
1	ED Assessment	Health NZ – Counties – ED	8,328
2	ED Assessment (Waitaha)	Health NZ – Canterbury – ED	4,881
3	ED Assessment HB primary emplate	Health NZ – Hawke's Bay – ED	3,424
4	ED Template v2	Health NZ – Whanganui – Hospc Sv	3,207
5	ED Template v2	Health NZ – Hawke's Bay – ED	2,875
6	ED Assessment	Health NZ – Whangarei – Hosp Svs	1,441
7	ED Assessment	Health NZ – Nelson Marl – ED	1,326
8	DN – Community and Clinic Ilot	Health NZ – Tairāwhiti – Hospc Sv	892
9	ED Assessment	Health NZ – Auckland – Hospc Sv	848
10	Ophthalmology Clinic Letter (Heidi)	Health NZ – Whanganui – Hospc Sv	644
11	ED Assessment	Health NZ – Taranaki – Hospc Sv	590
12	ED Template v2 (custom)	Health NZ – Whanganui – Hospc Sv	580
13	Child and Adolescent Psychiatric Review note	Health NZ – Canterbury – Hosp Svs	536
14	ED Assessment	Health NZ - Taupo - ED	508
15	TL ENT	Health NZ – Hawke's Bay – Hosp Svs	489

Weekly Session Count



Voice Style Distribution



Monthly Stats

	Report Date Month	Event Session Cou	Event Sign In Cou	Event Document Cou	Event Note Coun	Event Document + Not Coun	Event Minutes Transcribed Su	Event Ask AI Coun	Event Dictation Cou	Event Document by Ask AI Coun
1	Nov 2025	20,927	8,059	3,252	31,165	34,348	296,353.92	3,936	1,430	356
2	Oct 2025	11,786	5,915	1,958	18,934	20,824	149,115.85	2,278	514	142
3	Sep 2025	3,807	1,705	614	6,072	6,669	57,684.72	299	85	32
4	Aug 2025	2,801	805	539	4,271	4,798	46,915.18	181	64	16
5	Jul 2025	1,666	508	263	2,729	2,969	29,780.47	183	23	6
6	Jun 2025	1,160	444	364	1,933	2,291	19,690.18	244	14	0
7	May 2025	911	333	284	1,516	1,794	14,655.97	217	5	10
8	Apr 2025	204	63	97	352	447	4,832.18	62	0	10
9	Mar 2025	149	37	86	223	306	3,461.83	69	0	0
	Total	43,411	17,869	7,457	67,195	74,446	622,490.3	7,469	2,135	572

Health New Zealand
Te Whatu Ora

Health New Zealand | Te Whatu Ora

Heidi Health

Privacy Impact Assessment

Date 27/06/2025

Information for the Project

Health NZ | Te Whatu Ora is the kaitiaki and steward of a significant amount of Personal Information, including highly sensitive Health Information. We **all** have a responsibility to handle it appropriately and with care.

The best time to start privacy work (and this Privacy Impact Assessment) is **at the beginning** of your Project. By being proactive you can implement a privacy-by-design approach, prioritising privacy of Personal Information and ensuring you're upholding our obligations under the Privacy Act 2020 and Health Information Privacy Code 2020.

HNZ Privacy is here to support you in preparing this Privacy Impact Assessment. The complexity and scale of this Privacy Impact Assessment will depend on the complexity and scale of the Project. **We strongly recommend** you allow a **minimum** of 4-6 weeks to complete this Privacy Impact Assessment. For the more complex and significant Projects you should allow longer (including time to consult with the Office of the Privacy Commissioner as per their requirements). This Privacy Impact Assessment is not a last minute legal and privacy compliance checklist.

Please check out the "Guide to Completing a Privacy Impact Assessment" for more information.

The Project

Business Unit:	AI Laboratory – Planning, Funding and Outcomes
PIA Author:	Cheng Kai Jin
Date PIA prepared:	12/06/2025
Version number:	1.0
Project Go-live Date:	15/07/2025

Summary of Project / Change

Please **describe** the Project. This should include:

- What the purpose of the Project (or change)?
- What are the benefits and expected outcomes?
- Will it provide a solution to an existing problem?

Clinicians in New Zealand are at high risk of burnout with clinical administration being a large contributing factor. This challenge is not unique to New Zealand and is recognised globally as a significant pressure on the medical workforce. Heidi Health (Heidi) offers an AI-powered ambient scribe (AI scribe) solution designed to reduce this mental and administrative burden. Heidi can be activated during a consultation between a clinician and a patient, passively listening to the conversation. It generates transcripts which are then used to produce clinical notes, letters, and other documentation at the click of a button. Beyond individual consultations, the use of an ambient AI scribe has the potential to improve patient flow in high-demand settings such as emergency departments, where timely documentation is critical to ensuring patients are seen and treated within target timeframes.

Anticipated benefits of using the AI include:

- **Increased Efficiency:** Heidi reduces administrative burdens by aiding in the clinical documentation process, allowing clinicians to spend more time on patient care. This results in faster notetaking with minimal disruption to patient interaction.
- **Customization and Flexibility:** Heidi contains features to allow clinicians to create personalised templates and Heidi can be adapted to individual practice needs, ensuring output is tailored to each clinician's style and requirements.
- **Improved Workflows:** By integrating feedback from clinicians, Heidi is continuously optimised for workflow efficiencies, enhancing user experience and improving the documentation process.

- **Support for Diverse Clinicians:** Heidi is built to be language-agnostic and culturally adaptive, ensuring clinicians from various backgrounds can use it comfortably which aligns with our commitment to health equity.

Anticipated risks of using the AI:

- **Over-reliance on AI:** The speed and quality of AI-generated notes could lead to clinician over-reliance, with users potentially overlooking the need for review and verification. However, clinicians remain ultimately responsible for the accuracy and completeness of the clinical record. Heidi mitigates this risk through built-in prompts reminding clinicians to review and confirm generated content before finalising documentation. In addition, Health NZ will provide clinicians with training prior to the use of Heidi, ensuring that users are fully informed of these expectations and understand their ongoing responsibility for the integrity and accuracy of clinical documentation.
- **Privacy and Security Concerns:** There are concerns around how AI stores and processes data, especially highly sensitive patient data in clinical settings. However, Heidi adheres to strict security standards and has obtained relevant certifications (ISO27001 and SOC2 Type 2) to protect patient data. These security measures are designed to comply with the highest industry standards, ensuring that all patient information is handled with confidentiality and integrity.
- **Change Management and Adoption:** Heidi understands that new technological transformation is difficult and the importance of having vendor support is crucial in supporting sustained use. Heidi provides dedicated onboarding and ongoing support to facilitate smooth transitions and ensure that clinicians can leverage Heidi effectively. Their support system includes training resources, real-time assistance, and user guides to enhance user confidence and competence in using Heidi. NAIAEAG review will occur after generation of the PIA for this activity.

What is the Health NZ **scope** for your Project? *i.e., is the Project for a single District, Region, or the whole of Health NZ?*

The project has a broad scope, aiming to endorse the use of Heidi across Health NZ as a whole. While the specific use cases and clinical settings are not specified, this Privacy Impact Assessment is intended to provide general assessment to support the safe and controlled introduction of Heidi into Health NZ services. It will enable clinical teams to begin testing and evaluating the tool within their respective environments.

Will Health NZ be partnering with any individuals or agencies outside of Health NZ on this Project?
If so, who? What is each parties' role in this Project?

Heidi Health (vendor): Heidi Health is the primary vendor providing the platform, infrastructure, and ongoing support for the AI ambient scribe solution. Heidi Health will be responsible for the secure processing of personal information in accordance with applicable privacy and security requirements.

Hendrix Health (vendor partner): Hendrix Health is a vendor partner supporting the onboarding and implementation process. They will assist clinicians in the safe and effective implementation of Heidi within their practices, including providing training, change management support, and best practice guidance.

Please summarise:

- What information will be collected or handled by this Project?
- Where is the information coming from?

The project will collect, and handle information derived from clinical conversations between patients and clinicians during consultations. From a technology perspective, there are two steps for an AI Scribe solution:

1) First, the spoken content of the interaction is processed in real time to generate a transcript of the conversation.
2) Once a transcript is generated, a large language model is used to summarise the transcript into medical documentation. Although clinic letters is the primary documentation generated, Heidi will have the function to generate other medical documents (e.g. referral letters or discharge letters).

While Heidi processes the voice recording to support transcription, the audio is not retained and is automatically deleted after processing. The resulting AI-generated transcript and clinical documentation are subject to customisable retention settings, which can be defined by Health NZ in accordance with applicable governance and retention policies.

Heidi offers a highly flexible templating system that can be tailored to reflect the structure, language, and clinical communication style preferred by Health NZ, individual departments, or clinicians. Templates in Heidi are built using prompt engineering, allowing the underlying AI to generate structured, clinically relevant outputs in a predefined format — such as letters, progress notes, or discharge summaries.

Templates can be created in two main ways. First, Heidi's in-house medical knowledge team (comprising former clinicians and prompt engineers) can assist directly in building out templates based on real-world examples. In this approach, Health NZ or the requesting team would provide a sample letter, note, or ideal format (e.g., a referral letter or SOAP-style note), and the Heidi team will translate that structure into a functioning Heidi template using prompt engineering best practices. This is particularly helpful during onboarding or when high consistency across a department or service is required.

Second, clinicians also have the ability to create and customise their own templates directly within Heidi. Heidi supports this with a guided interface in the product and a comprehensive set of written resources that walk users through template creation at various levels of complexity — from basic setup to advanced optimisation. These resources are publicly available here:

- Getting Started with Templates
- Creating Templates: A Basic Guide
- Improving Your Templates: Intermediate Guide
- Mastering Templates: Advanced Guide

In practice, many clinicians start with Heidi's pre-built templates or examples, then customise them over time using the interface provided.

Please **advise** if the collection, use or sharing of information in this Project affects Māori interests.
If so- what are those interests? How are they affected? How will you accommodate them?[1]

Heidi recognises that Māori data is a taonga and that the deployment of digital tools in healthcare must uphold Te Tiriti o Waitangi obligations and reflect Māori worldviews. This has been a core consideration guiding Heidi's implementation in Aotearoa. In collaboration with Māori health and data sovereignty leaders from Health Hawke's Bay and Tu Ora Compass, Heidi has co-developed culturally grounded strategies that explicitly align with the principles of tino rangatiratanga, mana motuhake, kaitiakitanga, and whanaungatanga.

Heidi's implementation process for New Zealand has included Māori governance input and review. Regular hui has been held with Māori clinicians, iwi representatives, and data sovereignty advocates. These engagements have shaped key areas of the adapting the product for NZ's context, including:

- The creation of informed consent materials that speak to Māori concepts of autonomy and trust.
- The implementation of a policy of no use of Māori health data for model training
- The translation of all patient-facing materials into te reo Māori and ensuring support for macrons and special characters.
- Technical validation that Heidi accurately transcribes and reflects Māori names, dialects, and clinical phrases, continued improvement of translation accuracy of te reo Māori and Pasifika languages and continued steps to ensure Heidi utilise locally ethically sourced references where available.

Heidi has further aligned with the Te Mana Raraunga Māori Data Sovereignty Principles, including:

- **Mana Motuhake**: Ensuring Māori control over their data through informed consent processes and withdrawal rights.

[1] It is a requirement of our Government Chief Privacy Officer that this is addressed in our Privacy Impact Assessments.

- **Kaitiakitanga**: Protecting data as a sacred taonga with encryption, access controls, and transparent storage locations.
- **Whanaungatanga**: Maintaining respectful relationships with Māori communities through consistent consultation and feedback loops.
- **Kotahitanga and Equity**: Ensuring Heidi delivers community-wide benefits such as improved consultation time and record accuracy.
- **Tino Rangatiratanga**: Empowering Māori patients to opt in or out of Heidi use, consistent with their right to self-determination

Although Heidi's primary infrastructure currently uses ISO27001-certified cloud storage in Sydney, Heidi have committed to relocating this infrastructure to Aotearoa within the next 12 months as the infrastructure becomes available. This has been communicated openly with Māori leaders and is a priority under Heidi's cultural alignment roadmap. This ensures data is kept within a jurisdiction that upholds local tikanga and allows for enhanced oversight by Māori governance bodies.

Heidi is also working on developing local Māori data governance advisory panels for ongoing oversight. These panels will ensure that Māori are not excluded from decisions affecting their health data, and that the deployment of AI in clinical settings does not perpetuate structural biases or inequities. Additionally, clinical explainers and staff training through implementation partners at Hendrix Health include modules on Māori data sovereignty and culturally safe engagement.

Information Flow Diagram

Please insert a diagram (*if available from project documentation*) showing the end-to-end information flows relevant to this project.

Heidi is accessible through web, phone, and desktop applications. Each application utilises the same infrastructure, and the flow of data is consistent across platforms. Key areas of consideration in the information flow include:

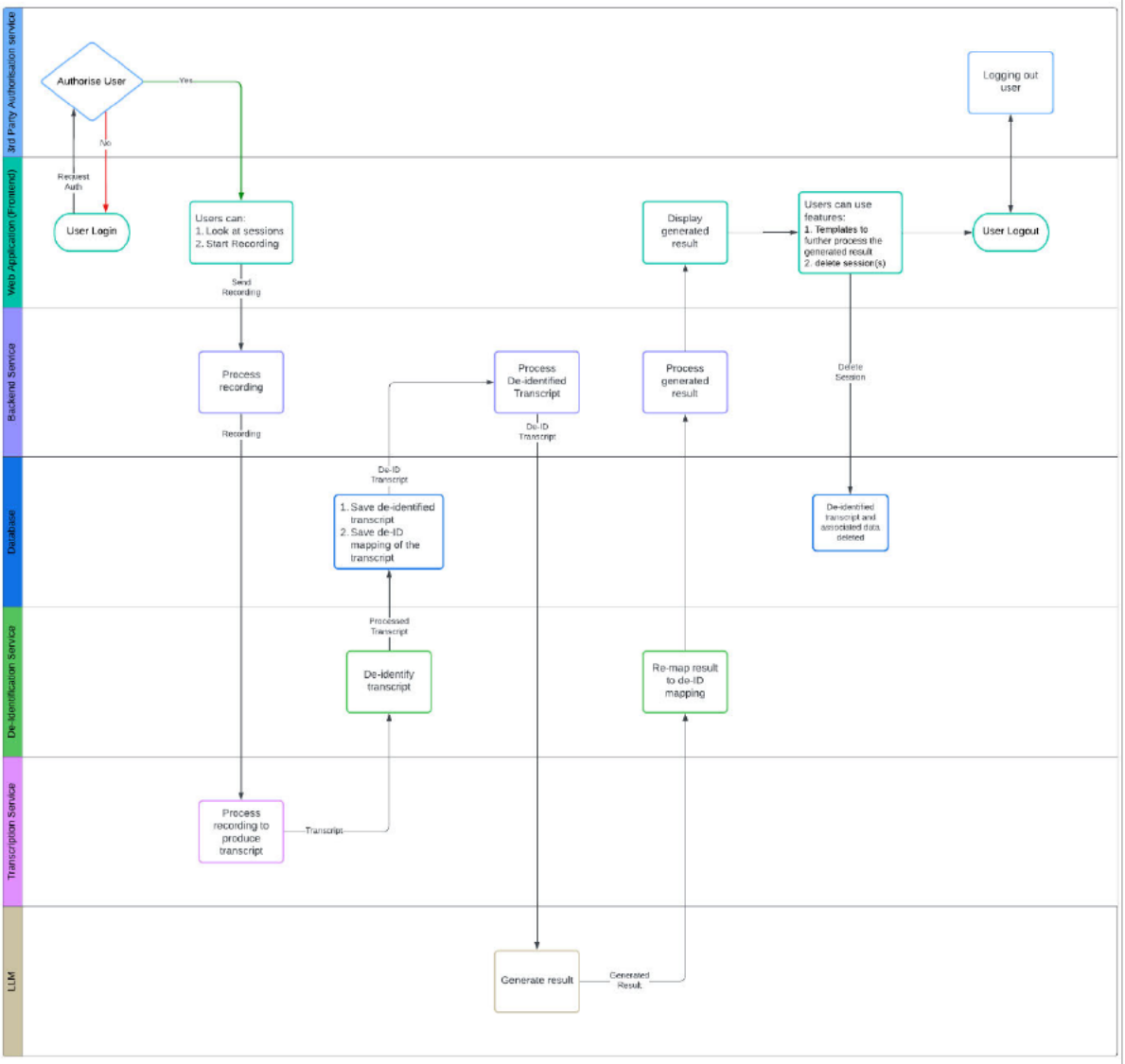
1) Voice to Text Transcription – At the conclusion of a clinical consultation, the recorded audio is processed into a transcript. This transcription occurs via a third-party speech-to-text service provider and is governed by Heidi through DPAs that prohibit secondary data use. Immediately following transcription, the original voice recording is permanently deleted and is never retained or stored. The transcript is then de-identified, with personally identifiable information such as patient names or locations replaced with placeholders (e.g. "Joe Deer" becomes "[Patient Name]").

2) Transcript to Clinical Note – The de-identified transcript is sent to large language models for summarisation into a draft clinical note. To ensure high quality output across various specialties, different LLMs may be used depending on the context or use case. Due to commercial sensitivity, specific LLM model types cannot be named however models from major LLM vendors such as Google and Anthropic have been utilised within Heidi's environment. All LLM providers utilised by Heidi operate under formal DPAs if necessary. These agreements strictly prohibit any form of secondary data use, including model training, and ensure compliance with privacy, security, and data governance standards expected by Health NZ.

3) Clinician Review and Modification – The draft clinical note is returned to the clinician within Heidi's user interface. Clinicians are required to review, edit, and approve the content before it can be finalised and transferred to the patient's health record. This human-in-the-loop approach ensures that clinicians remain accountable for the accuracy, completeness, and appropriateness of all documentation. In addition, if the draft output is of insufficient quality, clinicians can regenerate the note using tailored prompts or community configured templates.

4) Output and storage - Once the clinician approves the documentation, it can be transferred into the patient's clinical record system. Audio recordings are not retained at any point and are automatically deleted immediately after transcription. Transcripts and draft documents are stored with configurable retention settings defined by Health NZ.

5) Security and Data Hosting - All data managed by Heidi is encrypted both in transit and at rest, using industry-standard encryption protocols. Heidi's infrastructure is hosted on Amazon Web Services (AWS) servers located in Sydney, Australia. Access to data is strictly controlled, with audit logs in place to monitor access and ensure compliance with data governance obligations.



Scope of Assessment

Please define the scope of this PIA
The project has a broad scope, aiming to endorse the use of Heidi across Health NZ as a whole. While the specific use cases and clinical settings are not specified, this Privacy Impact Assessment is intended to provide general assessment to support the safe and controlled introduction of Heidi into Health NZ services. It will enable clinical teams to begin testing and evaluating the tool within their respective environments under appropriate oversight.
Please describe what has been excluded from the scope of this PIA and why
Specific clinical use cases have been excluded from the scope of this PIA. Instead, this PIA has been conducted to provide general endorsement for the use of Heidi within Health NZ, enabling clinical services

to begin testing the tool in defined environments. Separate assessments or governance steps may be undertaken as specific use cases are identified and progressed into broader clinical implementation.

Appendices

To finalise this PIA, you may need to provide your Privacy Officer with supplementary documents (*for example, a draft Privacy Statement, Information Sharing Agreement, Cloud Risk Assessment*). You can include these supplementary documents as **appendices** to this PIA.

If you have **added appendices** to this PIA, please list them here:

Appendices	Information
Appendix 1	Risk and Mitigation Table
Appendix 2	Glossary
Appendix 3	Te Whatu Ora AI Framework
Appendix 4	Click or tap here to enter text.

Assessment Questions

Does the project involve personal information?	YES	NO
	☒	☐

If you're unsure what personal information is, please see the "Guide to completing a Privacy Impact Assessment". For the purpose of this question, "***involve***" includes to collect, store, use, and/or disclose personal information.

- If the answer is '**No**' then there is no need to continue with this PIA. You **must** still complete a Privacy Threshold Assessment and email this to your Privacy Officer for approval.
- If the answer is '**Yes**', please move on to the next section (Health Information).

Does the project involve personal health information?	YES	NO
	☒	☐

The Health Information Privacy Code 2020 applies when a project handles health information. The Privacy Act 2020 applies when the project handles any personal information that is not health information. If you are unsure what personal information is, please see the "Guide to completing a Privacy Impact Assessment".

If your project does handle health information, as you work through the remaining sections in this PIA you should apply Rules 1 to 13 of the Health Information Privacy Code 2020 as they correspond to the 13 privacy principles.

Principle 1:
Lawful purpose and necessary collection of personal information

Principle 1 of the Privacy Act 2020 states that personal information **should not** be collected by any agency **unless** the information is collected for a **lawful purpose** connected with a function or activity of the agency, **and** the collection is **necessary** for that purpose.

⚠ The project should only collect the minimum amount of personal information that is necessary for the relevant function or activity ("data minimisation"). If the project **does not** require identifying information, then we **should not** collect it.

Please complete the following table:

List all information collected by project	Please state why this information is needed for the purpose of this project
Any patient data or information which might be discussed in a standard clinical consultation in various clinical settings including: • Name • Address • Phone number • Gender • Sexual orientation • Date of birth • Relationship status • Family and social history • Medical history	This information is collected during a clinical encounter and used to generate clinical notes and documents.

• Progress notes • Medications & prescriptions • Allergies • Diagnosis status • Lab orders & results • Disability data	
Practitioner information: Where you are a Practitioner, we may also collect information relating to your qualifications, registrations, training and educational background.	The privacy policy states that qualifications, registrations, training and educational background may be collected through Heidi or a third party. During the sign-up process, clinicians will need to provide the specialty and the country they work in. Additional collected information (e.g. qualifications, training etc) are likely originating from third parties.

Please state the lawful purpose for the collection of this personal information
Heidi collects health information solely for the purpose of supporting clinicians in the creation of clinical documentation. Heidi functions as an 'ambient scribe', converting spoken interactions between clinician and patient into draft clinical notes that can be reviewed, edited, and finalised by the clinician. The information collected is limited to what is spoken during the clinical interaction and is constrained by the scope of documentation typically required for clinical records, such as presenting complaint, history, findings, and management plans. No information is collected beyond what would ordinarily be captured in a manual consultation note, and Heidi is not used for clinical decision-making, diagnosis, or treatment recommendation. Heidi is designed to operate transparently in clinical settings, with all personal information collected directly from the individual and the clinician during a consultation with their clinician. The nature of the data collected is limited to what the patient voluntarily shares during the course of the clinical conversation. Heidi does not retain audio, and no data is collected passively or without the knowledge of the individual. The purpose of collection is clear and narrowly defined: to assist the clinician by generating a draft clinical note from the spoken interaction, which the clinician will then review, edit, and approve before it forms part of the formal medical record. Patients are not required to provide any specific information to Heidi — they are simply engaging in a clinical conversation as they normally would, and the scribe operates passively in the background to support the clinician's documentation. The purpose for collection is clearly defined and communicated to clinicians during onboarding, and is reflected in the product's documentation, privacy policy, and support materials. Importantly, this purpose does not change across jurisdictions. Heidi does not process the collected data for secondary uses such as marketing, AI training, or profiling. However, in certain situations, such as technical issues, Heidi may utilise transcript and AI output data to fix the identified issues. Frequency of this occurring is low and only occurs at request of Health NZ staff through the feedback function present in Heidi. In addition, Heidi enables clinicians and provider organisations to configure automatic deletion periods for temporary content stored within the system before it is permanently deleted, ensuring that only what is required for the stated purpose is retained. Within the HNZ context, the use of this technology for scribe activities within clinical settings is lawful under the Pae Ora Act s14(1)(b) which enables Health New Zealand to own and operate clinical services. This technology is used within these environments, and the information is collected as part of the requirements of HNZ's objectives and functions under this Act.

Collection of clinical information within a clinical interaction is both necessary to document that encounter to enable the ongoing management of the patient, but also under the requirements of the Health and Disability Services Commissioner Act 1994 and the Health Act 1956.

	YES	NO
Could the project use **aggregated or anonymised data** and still satisfy the project's purpose?	☐	☒
Is the project collecting **the minimum** amount of personal information required for the purpose of the project?	☒	☐

Please provide further information here if you're not using the minimum amount of personal information, or you could use aggregated or anonymised data
Click or tap here to enter text.

	YES	NO
Will the project be using cookies or other analytics?	☒	☐
If **yes**, please provide further information: Heidi's website includes pages that use cookies which are small files that store information on computers, mobile phones or other devices. Heidi may use them to recognise users across devices and browsing sessions. Users of Heidi can configure their internet browser to accept all cookies, reject all cookies or notify them when a cookie is sent. Heidi may also use third party analytics tools such as Google Analytics, Meta Pixel, Mixpanel, Braze or Segment to help gather and analyse information relating to users of their website and Platform.		

Compliance check with Principle 1

Does the project comply with Principle 1?	**YES**	**NO**	**UNSURE**
The information is collected for a lawful purpose and the collection is necessary for that purpose	☒	☐	☐

- Please complete Principle/Rule 1 of the Risk and Mitigation Tables (Appendix 1), summarising the actual/potential risks identified with this Principle, and outline the current controls, and/or recommendations to be implemented before continuing on to the next section.

Principle 2:
Collection directly from the individual concerned

Principle 2 of the Privacy Act 2020 requires an agency to collect information **directly** from the individual concerned unless an exception applies.

	YES	NO
Are you **only** collecting personal information **directly** from the individual?	☒	☐

- If you have answered "No", please answer the questions in this section

Please state why you're not collecting information directly from the individual
Heidi collects personal health information directly from the individual concerned, via the real-time conversation between the patient and their treating clinician. Heidi does not import data from external databases, electronic health records, or third-party sources without the clinician's instruction or action. All information is generated within the clinical consultation context, meaning there is a high level of assurance that the data is coming directly from the individual and is accurate in terms of origin and provenance. Heidi's system architecture is designed so that Heidi is used only at the point of care, in the presence of both clinician and patient, and under the clinician's control. Where information about the patient is mentioned by a third party (e.g., a family member present during the consultation), it is treated as secondary commentary unless confirmed and recorded by the clinician. There are no integrations that allow Heidi to independently pull health data from other systems such as laboratory systems or pharmacy records, which ensures that the platform cannot inadvertently collect third-party or mismatched information without clinical oversight. This approach is consistent with Principle 2 and Rule 2 of the Health Information Privacy Code, which establish that health information should be collected directly from the individual concerned unless one of the permitted exceptions applies. In Heidi's case, these exceptions are rarely, if ever, invoked, as the primary source of all content is the spoken conversation between the clinician and patient. In settings where multiple people may be present during the consult (e.g. whānau members, caregivers, or translators), clinicians are advised to ensure the patient understands that Heidi is documenting the consultation and that the final record will reflect what is spoken. Any use of prior notes or summaries from previous visits must be clinician-initiated and does not occur automatically.
Please state what legislative exception applies *The legislative exceptions can be found in Principle 2 of the Privacy Act and Rule 2 of the Health Information Privacy Code. If you're unsure if an exception applies, please contact the privacy team.*
Click or tap here to enter text.

Please complete the following table:

Information collected from third parties	Who is the third party?
Click here to enter text.	Click here to enter text.
Click here to enter text.	Click here to enter text.

Compliance check with Principle 2

Does the project comply with Principle 2?	YES	NO	UNSURE
Are you collecting directly from the individual concerned (or an exception applies)?	☒	☐	☐

- Please complete Principle/Rule 2 of the Risk and Mitigation Tables (Appendix 1), summarising the actual/potential risks identified with this Principle, and outline the current controls, and/or recommendations to be implemented before continuing on to the next section.

Principle 3:
Telling the individual what we are doing

Under Principle 3 of the Privacy Act 2020, when an agency collects personal information directly from individuals, there are certain things they **must** do **before** they collect the information or **as soon as practicable** after the information is collected. This includes making sure the individual is aware of:

(a) the **fact** that the agency is collecting personal information
(b) the **purpose** for which the agency is collecting the information
(c) the **intended recipients** of the information
(d) The name and address of the agency that holds the information
(e) the **consequences** (if any) if that individual does not provide that information
(f) whether the collection is **mandatory** or **voluntary**
(g) the **rights of access to, and request correction of,** the information.

There are only **limited circumstances** where we do not need to tell the individual the matters in (a) to (g) above.

	YES	NO
Will the project be telling an individual all the matters in Principle 3?	☒	☐

- If the answer is "**Yes**", please answer the questions in part A to C below only prior to completing the Principle 3 compliance check.
- If the answer is "**No**", please answer the questions in part D below only prior to completing the Principle 3 compliance check.

A. How you're going to tell the individual

Please describe how will you tell the individual how the project will manage their information. *For example, will you have a consent form, information leaflet, privacy statement etc?*
To ensure patients are aware that information is being collected and understand the purpose of that collection, Heidi provides privacy information in several accessible formats. Heidi will supply bilingual (English and Te Reo Māori) signage and patient information materials that clearly explain Heidi's role, the type of data being collected, and the clinician's ongoing responsibility for ensuring documentation accuracy. These materials are designed to be displayed prominently in the consultation space and waiting rooms. Patients will be directed to Heidi's website if patients require additional information. In addition to this passive notification, clinicians are trained to verbally explain that they are using Heidi to support documentation and that patients may request that Heidi is not used during their consultation. In these cases, clinicians can disable Heidi at any time.
Where will the document be made accessible? *For example, will it be published online? Link in an email? Hard copy?*
Signage and patient information materials will be available in clinical areas where the tool is being utilised, ensuring individuals are informed of its use. Clinicians will also receive education on the tool, including the requirement to obtain patient consent prior to use and the content to cover as part of the consent process.

Please include as an **appendix** a copy of any draft document that outlines how you will collect and handle an individual's personal information.

B. When you are going to tell the individual

Will you tell individuals before or after you have collected their information? If you're telling the individuals after you have collected their information, how long after?
Individuals will be informed and verbally consented to the use of Heidi prior to the start of the consultation with their clinician. As part of the consent process, individuals will be provided with information detailing how their data will be used and managed. Information regarding the content of the consent (e.g. data retention and no secondary data use) will be provided to clinicians during the onboarding process. Additional signage and patient information materials in clinical areas will further inform patients that Heidi is being used to support their care.

C. Mandatory or voluntary collection

Please state whether the collection of information is voluntary or mandatory?
The collection of information is mandatory in a healthcare setting, as clinicians are required to document patient encounters for clinical, legal, and continuity of care purposes. Heidi is a tool that supports and aids the documentation process; however, its use is voluntary. Patients may choose not to consent to the use of Heidi at any time before or during the consultation without affecting their access to care.
Please state to what extent, if any, the individual can opt out of providing some or all their information
Patients can opt out of the use of Heidi at any time, either before or during the consultation. While the documentation of the clinical encounter remains mandatory, individuals can choose not to have their information collected or processed through Heidi. In such cases, clinicians will continue to document the consultation manually using current methods.
Please state what happens if the individual does not want to disclose their information?
If an individual does not consent to the use of Heidi or does not wish to disclose their information through the tool, the clinician will proceed with manual documentation using current processes. The patient's care will not be affected by their decision. This decision will be made prior to the consultation.

D. Why you are not going to tell the individual

Please state why you are not telling the individual how the project will handle their personal information?
Click or tap here to enter text.
Please state what legislative exception applies? *The legislative exceptions can be found in Principle 3, Privacy Act 2020 and Rule 3, Health Information Privacy Code 2020*
Click or tap here to enter text.

Compliance check with Principle 3

Does the project comply with Principle 3?	YES	NO	UNSURE
Are you telling the individual how the project will handle their personal information (either before or as soon as practicable after the information is collected) or an exception applies?	☒	☐	☐

- Please complete Principle/Rule 3 of the Risk and Mitigation Tables (Appendix 1), summarising the actual/potential risks identified with this Principle, and outline the current controls, and/or recommendations to be implemented before continuing on to the next section.

Principle 4:
Fair and lawful collection of information

Principle 4 requires that when an agency collects information they must do so by lawful means **and** by means that, in the circumstances of the case are fair and not intrusive.

Your method of collection may be unfair, if it involves threatening, coercive, or misleading behaviour. What is fair also depends on the circumstances. You **need** to take particular care when collecting information from children and young people or other vulnerable groups. It may not be fair to collect information from children in the same manner as you would from an adult.

Please describe the current proposed method of information collection *If the information is not being collected fairly or lawfully, consider how the collection method could be adapted or modified to meet this Principle 4*
Heidi collects information in a manner that is lawful, fair, respectful, and not unreasonably intrusive. Heidi operates during active consultations between a clinician and patient and does not initiate recording or capture outside of that clearly defined session. The collection method is overt. Both the clinician and the patient are aware that the consultation is being transcribed to assist with clinical documentation. Patients are informed through prominently displayed signage, supported by verbal explanation from the clinician, that Heidi is in use. Consent is sought. These materials are designed to be culturally appropriate and are available in Te Reo Māori, Pacific languages, and plain English, ensuring accessibility and understanding across diverse populations, including those with low literacy or digital fluency. Patients are never coerced into participating. Heidi is configured so that clinicians can easily deactivate the tool if a patient expresses concern, confusion, or discomfort — ensuring that use of the platform is always respectful and responsive. No data is collected when Heidi is inactive, and the interface visibly indicates when it is enabled. Clinicians are also trained to take additional care when using Heidi in sensitive consultations (e.g. mental health, gender identity, sexual health) and are advised to confirm patient comfort explicitly. In these scenarios, Heidi remains optional, and declining to use it has no effect on the care the patient receives. This manner of collection aligns with the expectations of Rule 4 of the Health Information Privacy Code 2020 and Principle 4 of the Privacy Act 2020, ensuring that collection does not intrude upon the patient's reasonable expectations of privacy and is conducted fairly and transparently in the context of a healthcare relationship.
If you're collecting information from children or young people, **please state** what steps are you taking to address any power imbalance, and to obtain genuine consent for the collection (or authorisation) of their family/whānau?
Consent will be obtained prior to any information collection. For children or young people, consent will be required from a parent or legal guardian. In situations where they have capacity to consent for their own medical treatment, they will be consented to use Heidi. Individuals will be informed that participation is voluntary and may be withdrawn at any time without penalty.
If there are any cultural considerations, how you have assessed this, and, as appropriate, with whom you have consulted about how to ensure you collect the information in a culturally appropriate way
Answered in above question – 'Please **advise** if the collection, use or sharing of information in this Project affects Māori interests. If so- what are those interests? How are they affected? How will you accommodate them?'

Compliance check with Principle 4

Does the project comply with Principle 4?	YES	NO	UNSURE
Are you collecting information in a lawful manner and by means that are fair and not intrusive?	☒	☐	☐

- Please complete Principle/Rule 4 of the Risk and Mitigation Tables (Appendix 1), summarising the actual/potential risks identified with this Principle, and outline the current controls, and/or recommendations to be implemented before continuing on to the next section.

Principle 5: Storage and security

Principle 5 of the Privacy Act 2020 requires an agency that holds personal information to ensure that the information is protected by such **security safeguards that are reasonable** in the circumstances to take against loss, access, use, modification, disclosure, or other misuse

A. Cloud Computing Services

	YES	NO
Does your project/solution use any cloud-based services? Cloud services are infrastructure, platforms, or software that are hosted by third-party providers and made available to users through the internet.	☒	☐
Cloud-based services are required for the solution to function, as LLMs rely on cloud infrastructure to operate. Heidi has commercial data processing agreements with all third parties involved in the handling of data. These agreements are designed to ensure that no user data can be accessed, used, or stored by third parties beyond what is necessary for the specific purpose for which it was shared. Heidi also enforces zero retention policies with all third-party service providers. This means that after the necessary data processing tasks are completed, no data is retained, ensuring that patients' information cannot be reused or accessed for any other purpose. For New Zealand-based customers, all personal health information is stored exclusively on servers located in New Zealand or Australia. Data in transit and at rest is encrypted using AES-256 and TLS 1.2+ standards, and all access is logged, role-restricted, and monitored as part of Heidi's ISO/IEC 27001:2022 and SOC2 Type 2 certified security framework.		

B. Engaging with Information Security

	YES	NO
Have you engaged your relevant information security team for this project/solution?	☒	☐
Has the relevant information security team given its approval for this Project? *If the answer is "yes", please provide a copy of this approval to HNZ Privacy*	☐	☒
Please provide a further information: The project is undergoing a cyber security review, and the PIA can be conditioned based on their approval.		

Please contact your information security team for more information and support. Note that an SRA/ Cloud Service Provider Due Diligence Questionnaire may be completed concurrently with the PIA.

C. Storage

Please describe the system and location where the information is stored?
All data will be stored on our AWS servers hosted in Sydney, Australia. Heidi is committed to supporting New Zealand's data sovereignty principles and will migrate data processing and storage to New Zealand-based servers once suitable data centres have been established within New Zealand.

D. Access

Please state the roles that will have access to the personal information
In addition to this, Heidi staff may have access to personal data only after receiving explicit authorization from the user or NZ Health staff in order to rectify or solve a technical issue. The information accessed is de-identified to protect privacy, and any access by Heidi is logged meticulously. Access is restricted to a select number of internal Heidi staff members who are specifically authorized to handle this data, ensuring that it is controlled and monitored effectively. However, it must be emphasised that access is only conducted at the request of Health NZ staff and patient data is not routinely accessed by Heidi. Heidi also operates a structured quality assurance process focused on ensuring the reliability, accuracy, and consistency of clinical documentation outputs. This process does **not** involve access to real patient data unless explicitly approved by the provider for technical investigation. QA efforts instead rely on synthetic datasets, simulated vignettes, and feedback from implementation partners to evaluate model performance and adjust system behaviours. Outputs from the QA process are routinely reviewed by Heidi's in-house medical knowledge team (comprising of former clinicians), who evaluate system behaviour in edge cases, improve prompting structures, and refine templates. If any provider-initiated access to specific sessions is required for deeper technical assistance or support purposes, this is logged, access-controlled, and conducted only with authorisation.
Please describe why these roles need access to the personal information
Limited roles have access for technical quality assurance purposes (ie technical troubleshooting and improvement)
Please describe how access will be controlled or monitored? • Explain the process for granting user access and removing user access (including if someone leaves or changes roles) • Describe access controls (for example, role-based access)
Heidi utilises role based access and accounts will be set up to ensure that only the care team will have access to patient data.

Will access be controlled **by at least two-factor authentication**? The Office of the Privacy Commissioner has said that agencies may be in breach of the Privacy Act 2020 if they do not use at least two factor-authentication where applicable.	**YES**	**NO**	**NA**
	☒	☐	☐

E. Auditing Accounts

Please state: • if, and to what *extent*, the project can *audit* user access to the personal information • what will be audited, who will conduct the audit, how regularly the audit will occur etc

The identity of members of staff who have accessed an individual's information is personal information about that individual. This means this is something that individuals are entitled to request under the Privacy Act.

Privilege use and unauthorized access attempts are monitored through an audit trail. Heidi logs all access and actions taken by users, including the date, time, and details of the transaction. Alerts are configured to notify administrators of any unauthorized access attempts or unusual activity patterns.

F. Any other Information

Please state any other steps the project has taken/will take to prevent loss, misuse, unauthorised access, modification, or disclosure of personal information

For example:

- *Is information encrypted at rest and in transit? What other relevant safeguards are utilised during the transit of information?*
- *Is there a need for additional privacy training, new policies, processes, or contracts?*
- *How will you keep physical copies of documents secure?*
- *How will you ensure conversations are not overheard?*
- *What checks will be done to ensure you're talking to, and sharing information with, the right person?*
- *What are the security classification and any endorsements the information will have (for example, IN-CONFIDENCE, MEDICAL IN-CONFIDENCE etc)*
- *what backup processes is the project putting in place? Do they include backups of metadata (for example, audit logs)? Where are backups stored?*

Personal information is never stored longer than required to fulfil the purpose of documentation. Heidi enables clinicians and providers to select appropriate retention windows (e.g., 1, 3, 7, or 21 days) for temporary storage of consultation notes and transcripts. After this period, data is automatically and irreversibly deleted unless the note has been reviewed and saved into the Health NZ's clinical system.
Access to personal information is restricted to the clinician and authorised administrative staff within the healthcare provider's environment. Heidi staff do not access patient data unless explicitly requested for technical support and only under a signed support and confidentiality agreement. All access attempts are logged and auditable.

Heidi conducts regular penetration testing, vendor risk reviews, and incident response simulations. Subprocessors (e.g. AWS, authentication providers) are subject to Data Processing Agreements (DPAs) and are reviewed at least annually and listed transparently on their website (https://trust.heidihealth.com/subprocessors).
Heidi does not utilise personal or sensitive information for product development or AI training.

Compliance check with Principle 5

Does the project comply with Principle 5?	YES	NO	UNSURE
When the project holds personal information, is it using security safeguards that are reasonable to protect against loss, access, use, modification, disclosure, or other misuse?	☒	☐	☐

- Please complete Principle/Rule 5 of the Risk and Mitigation Tables (Appendix 1), summarising the actual/potential risks identified with this Principle, and outline the current controls, and/or recommendations to be implemented before continuing on to the next section.

Principle 6:
Access to personal information

Under **Principle 6** of the Privacy Act 2020 an individual has the right to confirm **if an agency holds personal information** about them, **and** if it exists, to have **access** to that information.

Access to personal information includes the right to ask who has accessed it (i.e., information from audit logs). If an individual is given access to their information, the individual must be advised that they may request correction of their information.

Please outline how individuals will be able to access their information. *For example, will it be through existing information request processes (for example, requests for clinical records), or will a new process need to be put in place?*
Patients have the right to access their personal information held within Heidi, although Heidi itself does not serve as the system of record. Once a clinical note is reviewed and finalised, it becomes part of the patient's clinical record. Patients may request access to this record via the current Health NZ processes. To support compliance with the Privacy Act 2020 and the Health Information Privacy Code 2020, Heidi ensures that: • All stored records are attributable to the user and timestamped • Requests for access can be made via the provider and supported by Heidi's platform if needed • Only authorised users with administrative access can view records. Clinicians will have their own individual accounts set up within Heidi which will contain the transcript and medical note for a preset period. Clinicians can access these notes, amend and transfer the document into the patient clinical record.
Please outline how you intend to ensure that it is possible to find the information about a specific individual?
Clinicians are responsible for creating the patient note and ensuring that the information generated by Heidi is incorporated into the patient's final medical record. Heidi allows clinicians to include the patient's name within each session, and each session is automatically timestamped to support later reference.

Compliance with Principle 6

Does the project comply with Principle 6?	**YES**	**NO**	**UNSURE**
Is there a process in place to ensure an individual can ask Health NZ if it holds personal information about them and the individual can access that information?	☒	☐	☐

- Please complete Principle/Rule 6 of the Risk and Mitigation Tables (Appendix 1), summarising the actual/potential risks identified with this Principle, and outline the current controls, and/or recommendations to be implemented before continuing on to the next section.

Principle 7:
Request to ask for correction of information

Under **Principle 7** of the Privacy Act 2020, where an agency holds information, the individual concerned is entitled to request correction of the information.

Please describe how an individual can ask to have their information corrected? *For example, will it be through existing processes, or will a new process need to be put in place?*
Heidi supports the right of individuals to request correction of their personal information by ensuring that all data captured through the platform remains editable and under the control of the clinician until it is reviewed, approved, and transferred into Health NZ's record system. Clinicians can modify, delete, or correct any part of the draft note or transcript within the Heidi platform during the active retention period. Once a note has been transferred out of Heidi into Health NZ's system, the ability to make further changes must follow the Health NZ's internal correction procedures.

Where the healthcare provider or clinician identifies an error in information generated by Heidi, whether flagged by a patient or discovered during review, they may request support from Heidi's team to retrieve, amend, or clarify the relevant session (within the configured retention window). Heidi maintains internal controls to facilitate this process and ensures timely responses to such correction requests in compliance with Rule 7 of the Health Information Privacy Code 2020 and Principle 7 of the Privacy Act 2020.

To promote patient equity and engagement in their own health outcomes, Heidi also supports the ability for clinicians to share the generated note with the patient during or after the consultation. Patients may ask their clinician to view what Heidi has transcribed, and clinicians are encouraged to review this with the patient as part of good documentation practice and shared decision-making. This increases transparency and reduces the risk of miscommunication or missed content, especially in culturally sensitive or complex consultations.

Please outline how you intend to ensure that it is possible to find the information about a specific individual and to correct it (or add a statement of correction) if required?

Clinicians are responsible for documenting their interactions with patients and for ensuring that the correct clinical note is associated with the correct patient record. In situations where an error occurs, such as a note being incorrectly attributed to the wrong individual, standard Health NZ processes for correction of health information will apply.

Please outline how a statement of correction provided by that individual will be managed so that it is always able to be viewed together with the disputed information.

For example, does your proposed system have the capacity to link or attach a statement of correction to a person's file?

Heidi is used to generate an initial draft documentation. Clinicians are responsible for reviewing the draft, ensuring its accuracy, and incorporating it into the finalised patient record. Heidi itself does not store or maintain finalised clinical records. In the event that an error is identified after documentation has been finalised, standard Health NZ processes for correcting clinical documentation will apply.

Compliance check with Principle 7

Does the project comply with Principle 7?	YES	NO	UNSURE
Is there a process in place to enable an individual to request the correction of their personal information?	☒	☐	☐

- Please complete Principle/Rule 7 of the Risk and Mitigation Tables (Appendix 1), summarising the actual/potential risks identified with this Principle, and outline the current controls, and/or recommendations to be implemented before continuing on to the next section.

Principle 8:
Accuracy of personal information before it is used or disclosed

Principle 8 of the Privacy Act 2020 states that an agency must not use or disclose information without taking reasonable steps to ensure that the information is accurate, up to date, complete, relevant, and not misleading.

⚠ If you're not collecting information directly from the individual, or are relying on old records, (as examples) there is a risk that the information will not be accurate or up to date. Carefully consider the consequences for individuals if the personal information is not accurate or up to date.

How will you ensure that only **accurate, up to date, complete and relevant** information is acted on?

All information generated by Heidi is presented as a draft and must be manually reviewed, edited, and approved by the clinician before it can be saved to the patient's record. Heidi does not allow direct auto-population of electronic health records, providing a safeguard against transcription errors, misinterpretations, or the inclusion of irrelevant content from casual conversation. As part of the onboarding process, clinicians will be instructed to review and verify the output for accuracy, completeness, and relevance before finalising the clinical documentation into a patient's record.

This step aligns with Rule 8 of the Health Information Privacy Code and Principle 8 of the Privacy Act, which require agencies to ensure personal information is accurate and not misleading before being used. Heidi supplements this by:

- Timestamping the original session,
- Allowing edits and deletions
- Preventing finalisation of notes without clinician interaction.

Furthermore, as part of the onboarding process, clinicians are trained to ensure that summaries are comprehensive, reflect the key clinical elements of the interaction, and exclude personal commentary, unrelated dialogue, or speculative content. These safeguards are especially important given the risk of conversational language being misinterpreted or taken out of context in ambient transcription

Heidi has been working with local Māori communities to improve Te Reo understanding. Current performance is unknown, and clinicians will be reminded of the limitation during onboarding and highlight the importance to double check the AI output prior to finalisation of the document.

Compliance check with Principle 8

Does the project comply with Principle 8?	YES	NO	UNSURE
Does the project ensure that information is accurate, up to date, complete and relevant before the information is used?	☒	☐	☐

- Please complete Principle/Rule 8 of the Risk and Mitigation Tables (Appendix 1), summarising the actual/potential risks identified with this Principle, and outline the current controls, and/or recommendations to be implemented before continuing on to the next section.

Principle 9:
Do not keep information longer than necessary

Principle 9 of the Privacy Act 2020 states that an agency that holds personal information must not keep that information for longer than is required for the purposes for which the information may lawfully be used.

⚠ Principle 9 (*and rule 9 of the Health Information Privacy Code)* does not apply in a vacuum. There may be other rules and regulations that will specify how long certain information must be kept for (*for example, Public Records Act 2005)*. Once those other legislative requirements for retention have been met, then under Principle 9 (*or Rule 9)* the information should be disposed of when it is no longer needed for the project. We strongly recommend you engage your Records Manager to ensure records are managed consistently with the relevant general/functional disposal authority.

Please state how long the information will be held by Health NZ

Heidi follows a strict data minimisation and retention policy. The platform only retains personal health information for as long as is necessary to support the stated purpose of providing clinical documentation support. Once a note has been reviewed and exported to Health NZ's system, any remaining transcript or draft note on Heidi's platform is automatically deleted after a Health NZ configured retention window (e.g. 1, 3, 7, or 21 days).

Heidi also supports early deletion where required — for example, if a patient opts out during the consultation or requests removal of a specific session. Deleted data is irretrievably erased using secure, industry-standard deletion protocols. No audio is ever stored, so no retention schedule applies to the raw conversation itself. Importantly, the finalised notes are subject to the Public Records Act 2005 and will be stored by Health NZ accordingly. Heidi plays no role in long-term clinical record storage beyond the initial transcription support window. All retention settings are auditable and configurable at the provider level, and audit logs are maintained to demonstrate compliance. Heidi does retain some de-identified information as outlined in their privacy policy, "We may de-identify your general personal information and use it in aggregate form to conduct analysis on how our website, Platform and other services are being used to help us improve our services and provide benefits back to our users."
Please **state** the applicable legal requirements for retention of information (if any). *For example, Health (Retention of Health Information) Regulations 1996, Public Records Act 2005, General Disposal Authority 6, Functional Disposal Authority 1.*
The legal requirements for the retention of transcript data generated by Heidi are not yet fully determined, and formal legal advice will be sought as part of the implementation process. Heidi does not store transcripts indefinitely by default. If required, a process for the appropriate transfer, retention, and secure storage of transcript data will need to be developed in alignment with Health NZ policies, legal requirements, and best practice standards for health information management.
Please state: • whether all the personal information needs to be retained by the project • whether the information needs to be retained in a form that identifies the individual (*can it be retained in a de-identified manner)*
Heidi employs de-identification and pseudonymisation methods on all transcripts before they are processed and used to generate clinical notes. Heidi only retains de-identified and pseudonymised transcripts, clinical notes, and documents.
Please state: • how the information will be disposed of • who is responsible for ensuring disposal occurs
Heidi is responsible for ensuring data disposal occurs. Digital data will be permanently deleted from all systems and backups using secure data erasure methods. Heidi will ensure that third-party service providers follow similar secure data destruction protocols and provide verification, maintaining records of these activities.

Note: We also recommend:

1. **prior** to disposing of any the information, that you engage your Records Manager,
2. subject to the advice of your Records Manager, you keep a list of what has been disposed of and under what general/functional disposal authority.

Compliance check with Principle 9

Does the project comply with Principle 9?	YES	NO	UNSURE
Subject to satisfying any records management requirements, personal information is only retained for as long as it is required for the purposes of the project	☒	☐	☐

- Please complete Principle/Rule 9 of the Risk and Mitigation Tables (Appendix 1), summarising the actual/potential risks identified with this Principle, and outline the current controls, and/or recommendations to be implemented before continuing on to the next section.

Principle 10:
Limits on use of personal information

Principle 10 of the Privacy Act 2020 requires that an agency which obtains personal information for one purpose **must not** use the information for any other purpose **unless** the agency believes on reasonable grounds that an exception applies.

The Office of the Privacy Commissioner recommends keeping in mind the "no surprises test"- would the way in which you're planning to use the personal information come as a surprise to the person you collected it from?

Please describe how the information will be used in this project?

For example, if we are using information to assess an individual's eligibility to deliver a service, outline what information is being used for assessing the eligibility and what is required to deliver the service.

Heidi enforces strict limits on the use of personal information and complies fully with Rule 10 of the Health Information Privacy Code 2020 and Principle 10 of the Privacy Act 2020. The personal information collected by Heidi is used solely for the purpose of supporting clinicians in generating clinical documentation during consultations. It is not used for any secondary, unrelated, or commercial purposes.

To be unequivocal: Heidi does not, under any circumstances, use personal or sensitive health information to train AI models, develop new product features, or conduct internal analytics for system improvement. No identifiable or pseudonymised data from patient interactions is used for algorithm refinement or technical training. There is no automated or background use of health data for any form of model learning or optimisation. Furthermore, Heidi does not sell, share, or otherwise monetise user data, nor is any data shared with third parties for advertising, marketing, research, or other secondary purposes.

This position is not only embedded in Heidi's product design, but also clearly articulated in our publicly available Privacy Policy, which explicitly states that we do not use personal data to train our AI models or for any purpose other than providing our documentation support services. This ensures that users — both clinicians and patients — have transparency and assurance about how their data is handled.
The only permitted uses of personal information outside the core clinical documentation workflow are:

1. **Voluntarily submitted feedback**: When users intentionally provide session context (e.g., screenshots or note samples) in the course of requesting support or suggesting improvements. For clarity, the voluntary feedback mechanism within Heidi — such as the 1–5 rating (smiley face) feature — collects only high-level satisfaction scores and the userID, and does not transmit session content, transcripts, or clinical notes back to Heidi's team. No data is reviewed or accessed automatically during feedback submission. If a clinician wishes to raise a support ticket that involves specific note content or transcripts, this must be submitted manually and with explicit user awareness.
2. **Provider-requested internal analytics**: Where healthcare organisations request access to aggregated metrics (e.g. number of sessions per user) for their own reporting or workflow analysis. These metrics are generated from operational metadata only — no clinical or patient data is involved.

These uses are entirely optional, controlled, and consent based. No data is collected or reused without the clear and informed action of the user or Health NZ. All third-party sub processors (such as infrastructure and authentication providers) are bound by contractual DPAs that prohibit any form of secondary use, model training, or unauthorised data access. These sub processors are audited and reviewed regularly to ensure compliance.

	YES	NO
Are the uses listed above consistent with the purposes of collection you have outlined in Principle 1?	☒	☐
If the answer is "**No**", **please state** what legislative exception applies. *The legislative exceptions can be found in Principle 10 of the Privacy Act or Rule 10 of the Health Information Privacy Code. If you're unsure if an exception applies, please contact the Privacy team.*		
Click or tap here to enter text.		

	YES	NO
Does the use of information by the project involve information matching or sharing?	☐	☒
If the answer is "**yes**", please provide more information here. *Please consider any additional issues that may arise (for example, the need for agreements to enable and regulate matching and sharing).* Please annex any relevant documents to this PIA.		
Click or tap here to enter text.		

Compliance check with Principle 10

Does the project comply with Principle 10?	YES	NO	UNSURE
Will the personal information only be used for the purpose it was obtained or an exception applies?	☒	☐	☐

- Please complete Principle/Rule 10 of the Risk and Mitigation Tables (Appendix 1), summarising the actual/potential risks identified with this Principle, and outline the current controls, and/or recommendations to be implemented before continuing on to the next section.

Principle 11:
Limits on disclosure of personal information

Principle 11 of the Privacy Act 2020 states that an agency must not disclose the information unless the agency believes on reasonable grounds that an exception applies.

⚠ The Office of the Privacy Commissioner recommends keeping in mind the "no surprises test"- would the way in which you're planning to disclose the personal information come as a surprise to the person you collected it from? Please note that **principle 11 does not limit** storing personal information in "the cloud" or sharing information with a service provider that stores or processes information on our behalf.

	YES	NO
Will the project disclose personal information to individuals or agencies outside of Health NZ?	☒	☐

- If you have answered "**Yes**", please answer the following questions.

Please state the basis for disclosing personal information *The grounds can be found in Principle 11 of the Privacy Act or Rule 11 of the Health Information Privacy Code. If you're unsure if an exception applies, please contact the Privacy team.*

Heidi is designed to operate within a closed environment in which disclosure of personal information to third parties does not occur by default. Personal information processed through Heidi, including draft notes, consultation transcripts, and session metadata, is accessible only to the treating clinician and designated, authorised personnel within the Health NZ. Heidi itself, as the service provider, does not access or disclose data unless specifically authorised to do so for the purposes of providing technical support or where required by law.

Patients are informed through clinic materials (e.g. patient information sheets and posters) and consent process that Heidi will be used to support clinical documentation. These materials explain that the clinician retains full control of all information generated and that no information will be disclosed beyond the provider without consent. In line with Rule 11 of the Health Information Privacy Code and Principle 11 of the Privacy Act 2020, Heidi does not disclose any information externally without legal authority, patient consent, or a formal request from the provider. This includes disclosures to other health providers, government agencies, or legal entities.

From the clinician's perspective, Heidi requires the practitioner's name and area of work during account set up. None of this information will be disclosed by Heidi to third parties.

Where a disclosure is required by law (for example, under subpoena or court order), Heidi follows a structured process that involves notifying the healthcare provider, verifying the legitimacy of the request, and ensuring that only the minimum necessary information is disclosed. However, due to Heidi's data lifecycle settings, any personal information that has already been deleted following the provider's configured retention period is technically unrecoverable. Once deleted, the data is permanently and irreversibly erased and cannot be retrieved in response to any disclosure request — legal or otherwise. This approach helps limit unnecessary exposure and reduces the risk of retrospective access to sensitive information.

Heidi also maintains a public list of sub processors at https://trust.heidihealth.com/subprocessors, which outlines all infrastructure providers and services that may process data on Heidi's behalf. These sub processors do not access content or transmit data beyond their strictly defined role (e.g., cloud storage, authentication). All sub processors are bound by legally enforceable Data Processing Agreements (DPAs) that prohibit them from using, disclosing, or analysing personal data for any purpose other than providing the contracted service. They are not permitted to access, use, or share data for any secondary or unrelated function, including analytics, training, or profiling.

Patients are not asked to consent to any disclosure because no disclosure occurs unless they request it or it is required for continuity of care — in which case it is managed through the healthcare provider's existing health information release policies. Heidi never acts as a controller or decision-maker in those cases; the disclosure is initiated and managed solely by the healthcare provider.

If there is a disclosure to someone **other than the individual concerned, please:**

- list all parties that you will disclose the information to
- explain why those third parties need the information
- outline what safeguards will be put in place to ensure that the information is secure once it has been shared with the third party

Please see above.

Compliance with Principle 11

Does the project comply with Principle 11?	YES	NO	UNSURE
Personal information is not disclosed to an individual or agency outside of Health NZ or an exception applies	☒	☐	☐

- Please complete Principle/Rule 11 of the Risk and Mitigation Tables (Appendix 1), summarising the actual/potential risks identified with this Principle, and outline the current controls, and/or recommendations to be implemented before continuing on to the next section.

Principle 12:
Disclosure of information outside of New Zealand

Principle 12 of the Privacy Act provides that an agency may only disclose personal information to a foreign person or entity (B), if:

- The individual authorises it in situations where B may not be able to protect the information to the same degree as a NZ entity would; or
- B carries on business in NZ and is therefore subject to the Privacy Act 2020; or
- B's privacy laws offer comparable safeguards to the NZ Privacy Act 2020; or
- B is bound by contract or agreement to protect the information with similar safeguards to NZ standards.

⚠ Please note that **principle 12 does not limit** storing personal information in "the cloud" or sharing information with a service provider that stores or processes information on our behalf

	YES	NO
Will Health NZ disclose personal information to a foreign person or entity?	☒	☐

- If you have answered "**Yes**", please answer the following questions.

Please state:

- The foreign entities or persons that we will be disclosing personal information to
- Where the foreign entities or persons are based (i.e., which jurisdiction)
- Why the foreign entity or person needs to have the personal information
- what evidence you have that the foreign entity receiving information has the same safeguards available to protect the information as are provided under the Privacy Act 2020.
  - If the foreign entity cannot provide the same safeguards, indicate whether that has been explained to the individual, what has been explained and whether the individual consents to the sharing of their information with the foreign entity. Please provide evidence of that consent.
- Provide details on what safeguards have been put in place to protect the individual's information (such as a contract or an agreement with the foreign entity).
- Has an ethics or research committee, such as Health and Disability Ethics Committee, approved overseas disclosure?

All processing of personal health information for New Zealand customers occurs exclusively in Australia, in line with data residency expectations under the Health Information Privacy Code and the Privacy Act 2020. No personal or health data is processed, routed, or stored in any other jurisdiction. Heidi uses Australian-based cloud infrastructure that is ISO27001 and SOC2 Type 2 certified, and data is encrypted in transit and at rest at all times. We note this is not considered disclosure under the Privacy Act.

Where a disclosure is required by law (e.g. subpoena or formal request), Heidi will only comply after verifying the legitimacy of the request and consulting the healthcare provider. However, where data has already been deleted based on the provider's configured retention window, it is technically unrecoverable — deleted data cannot be retrieved even under legal demand, further limiting disclosure risk.

Heidi maintains a public list of all sub processors and infrastructure partners at https://trust.heidihealth.com/subprocessors, including their roles and geographic boundaries. All sub processors are bound by strict Data Processing Agreements that prohibit any form of secondary use or unauthorised disclosure of data. These sub processors do not access or transmit data beyond the defined scope of service delivery (e.g. secure storage, login authentication).

Patients are not asked to consent to any disclosure because Heidi does not disclose their information to any external party. Where onward disclosure is required for continuity of care (e.g. sharing the note with another

provider), this is handled solely by the clinician or provider organisation under their standard protocols. Heidi plays no role in such transactions and does not control or initiate disclosures.

Compliance check with Principle 12

Does the project comply with Principle 12?	YES	NO	UNSURE
Personal information is not disclosed outside of New Zealand, or it is authorised under Principle 12	☒	☐	☐

- Please complete Principle/Rule 12 of the Risk and Mitigation Tables (Appendix 1), summarising the actual/potential risks identified with this Principle, and outline the current controls, and/or recommendations to be implemented before continuing on to the next section.

Principle 13: Creation or use of unique identifiers

Principle 13 of the Privacy Act 2020 says an agency may only **assign** a unique identifier to an individual if that identifier is necessary to enable the agency to carry out 1 or more of its functions effectively.

To avoid doubt, Health NZ does not assign unique identifiers when it records and uses a unique identifier so that we can communication with another agency about the individual (please see IPP13(3) and Rule 13(5).

Please see "Guide to completing a Privacy Impact Assessment" for more information on unique identifiers.

	YES	NO
Will the project **assign** unique identifiers?	☐	☒
Will the project **use** unique identifiers?	☐	☒

- If you have answered "**Yes**" to any one of these questions, please answer the following questions

Please explain:

- What unique identifiers will be assigned or used for this project
- How will the unique identifiers be created?
- If you are proposing to use NHIs, can the project's purpose be achieved by using an alternative unique identifier
- Are you intending to use a unique identifier that has been assigned by another agency? If so, please consult the Privacy team.

In the case of Heidi, the assignment of unique identifiers is not relevant, as the product does not assign unique identifiers to individuals. The AI scribe uses clinicians' email addresses as unique logins for authentication purposes, which are already existing identifiers within the healthcare provider's systems.

Moreover, as the AI scribe is not currently integrated with any EHR systems, it does not assign or use unique identifiers for patient data within those systems. Any data processed by the AI scribe is tied to the clinical encounter rather than being associated with a unique identifier assigned by Heidi Health.

Compliance check with Principle 13

Does the project comply with Principle 13?	YES	NO	UNSURE

Does the project comply with Principle 13/ Rule 13 regarding the assignment and/or use of unique identifiers?	☒	☐	☐

- Please complete Principle/Rule 13 of the Risk and Mitigation Tables (Appendix 1), summarising the actual/potential risks identified with this Principle, and outline the current controls, and/or recommendations to be implemented before continuing on to the next section.

Artificial Intelligence
Initial Assessment

The Privacy Act 2020 applies to the use of Artificial Intelligence (**AI**). There is no single, universally accepted definition for AI. For the purposes of this PIA, we use the definition of the Office of the Privacy Commissioner- *"AI refers to computer systems doing tasks that seem like intelligent behaviour, such as finding patterns, putting items into categories, and triggering actions based on information", including:*

- ***machine learning systems** developed or refined by processing training data.*
- ***classifier systems** used to put information into categories (e.g., captioning images).*
- ***interpreter systems** that turn noisy input data into standardised outputs (e.g., deciding what words are present in speech or handwriting).*
- ***generative systems** used to create text, images, computer code, or something else.*
- ***automation** where computers take on tasks that people have done up until recently.*[2]

Use of Artificial Intelligence at Health NZ	YES	NO
Does your project/solution involve the design, development, deployment, and/or use of any form of **AI**?	☒	☐

If you have answered '**yes**' to this question, please complete the AI row of the Risk and Mitigation Tables (Appendix 1), and then complete the "**Artificial Intelligence – Privacy Assessment**". Please contact the Privacy team for more information.

Please note that in addition to engaging with HNZ Privacy on the use of Artificial Intelligence it is critical you also engage with other relevant stakeholders as applicable. HNZ Privacy approval of the use of Artificial Intelligence does not cover approvals from other relevant stakeholders.

Third Party Artificial Intelligence	YES	NO
Has your project been asked to **share** information that Health NZ holds (including personal or health information) with a third party to enable the third party to design, develop, train and/or deploy their own AI?	☐	☒
If Health NZ will contract with a third party for this project/ solution, do the contract terms/ Terms of Service etc allow the third party to use Health NZ information to develop, train and/or deploy their own AI?	☐	☒
If the answer is **'yes'** to either of these questions, please provide additional information:		

Once you have completed this section (Artificial Intelligence), please move on to the next section (Privacy Policies and Terms of Service).

[2] Office of the Privacy Commissioner- Artificial intelligence and the Information Privacy Principles, September 2023.

Privacy Policies and Terms of Service (or other contractual provisions)

If the Project is engaging anyone outside of Health NZ to provide services as part of this Project, please answer the following questions:

Third Party Privacy Policy/Statement	YES	NO
Has the Project reviewed the current Privacy Policy/Statement of the third party?	☒	☐
If the Project identified any privacy risks, mitigations, or controls from its review of the Privacy Policy/Statement, have these been documented and addressed in this Privacy Impact Assessment?	☒	☐
If you have answered "**no**" to either of these questions, please provide additional information:		

Terms of Service (or other contractual provisions)	YES	NO
Has the Project reviewed the relevant Privacy clauses in the Terms of Service (or other contractual provisions as applicable)?	☒	☐
If the Project identified any privacy risks, mitigations, or controls from its review of the relevant Privacy clauses in the Terms of Service (or other contractual provisions as applicable), have these been documented and addressed in this Privacy Impact Assessment?	☒	☐
Have you engaged HNZ Legal on a review of the relevant contractual provisions?	☒	☐
If you have answered "**no**" to any of these questions, please provide additional information:		

Once you have completed this section, please move on to the next section (Review and sign off).

Review and Sign Off

Conditional Approval	YES	NO
Are you seeking **conditional approval** of this Privacy Impact Assessment? *For example, if the Project does not have an approved Authority to Operate and it needs one from Information Security, you may ask for conditional approval until such time as one is in place.*	☐	☒

If you are seeking conditional approval, please state why:

All conditions in prior conditionally approved PIA met as of 1.10.25 and reviewed by Privacy Advisor.

If you are seeking conditional approval, please note that you **must**:

- Inform HNZ Privacy as soon as the condition has been met; and
- Update this Privacy Impact Assessment as required when the condition has been met

National Privacy Office

This is a conditional approval, there is a requirement for the cyber security review, development of a set of agreeable DPA terms and legal advice around retention period obligations. Once these terms have been met return the PIA to privacy for final sign off.

Name: Viv Kerr – Head of Privacy Signature: Viv Kerr	Date: 30/06/2025

National Privacy Office

This PIA was conditionally approved on 30.06.2025 with a requirement for the cyber security review, development of a set of agreeable DPA terms and legal advice around retention period obligations. As of this date, I understand these requirements have been met.

Name: Sarah Burr – Privacy Officer Signature: Sburr	Date: 02/10/2025

Business Owner

I approve this Privacy Impact Assessment, accepting that:

- I am accountable for the appropriate management of Personal Information associated with this initiative/system
- I am responsible for ensuring identified mitigations are actioned, and
- I own the privacy risks associated with this initiative/system.

Name: NAME – Health NZ ROLE Signature: Hopley	Date: 30/06/2025

Project Manager

I endorse that this Privacy Impact Assessment accurately and comprehensively describes the relevant parts of the initiative/system to be assessed and that all substantive privacy risks have been identified, along with appropriate mitigations to address these.

Name: Dr Cheng Kai Jin – AI Laboratory Clinical Director Signature: 	Date: 30/06/2025

Appendix 1: Risk and Mitigation Tables

- The risk and mitigation tables aim to help identify, describe, and mitigate actual and potential privacy risks involved in your project.
- For "**privacy risk description**", please identify each vulnerability associated to the Privacy Principle you are assessing.
- If there is more than one identified risk for a Principle/Rule, copy the relevant Principle/Rule ROW, and paste under the copied row and amend Reference No's. (see 'Guide for Completing a Privacy Risk Assessment' for examples)

Current Overall Risk Rating *As assessed by Health NZ - National Privacy Office*	Current Overall Risk Rating: Choose an item. Date: Click or tap to enter a date.
Target Risk Rating *Obtainable Risk Rating when recommendations implemented (outcome of Target Risk Rating Table)*	Target Risk Rating: Choose an item.

Reference No.	Privacy Principle or Rule	Risk Description	Current Controls	Current Risk Rating	Recommendations to further mitigate risk	Target Risk Rating			Owner	Date
	Principle or Rule being assessed	*Description of potential/actual risk*	*Controls currently in place which mitigate the risk*	Risk Rating	*Recommendation to mitigate residual risk*	Probability	Consequence	Risk Rating	*Role/area responsible for implementing*	*Date recommendation to be implemented by*
R.01	**Nil**	Change of process/ functionality after go-live and throughout the life of the Project, affecting the PI/HI involved.	National Privacy Office PIA/PTA Library	**Low**	The project will review and update this Privacy Impact Assessment whenever there is a chance to how personal information is collected, stored, accessed, used, disclosed, or otherwise handled. The Project team will proactively review this PIA every 12 months after the month of go-live, to ensure it is still accurate and up to date.	**Rare**	**Minimal**	**Low**		Every 12 months following project go live
R.02	**Principle/Rule 1** Collection is for a lawful purpose, and is necessary for that purpose			Select		Select.	Select	Select		
R.03	**Principle/Rule 2** Information is collected directly from individual			Select		Select.	Select	Select		
R.04	**Principle/Rule 3** Individual is aware of collection	That consent materials are not circulated or implemented appropriately in use settings.	Materials exist. Mandatory training for clinicians using this technology with HNZ endorsement for consent conversations.	**Low**	Where formal roll out occurs, standardised awareness programmes and/or information artefacts are designed for both patients and clinicians. There is formal responsibility for oversight of consent training at HNZ agreed implementation (ie if a service implements)	**Rare**	**Minimal**	**Low**	CK Jin	30 December 2025
R.05	**Principle/Rule 4** Collection is done in a lawful, fair and unintrusive way			Select		Select.	Select	Select		
R.06	**Principle/Rule 5** Storage and Security of information			Select		Select.	Select	Select		

Reference No.	Privacy Principle or Rule	Risk Description	Current Controls	Current Risk Rating	Recommendations to further mitigate risk	Target Risk Rating			Owner	Date
	Principle or Rule being assessed	*Description of potential/actual risk*	*Controls currently in place which mitigate the risk*	Risk Rating	*Recommendation to mitigate residual risk*	Probability	Consequence	Risk Rating	*Role/area responsible for implementing*	*Date recommendation to be implemented by*
R.07	**Principle/Rule 6** Individual can access their information			Select		Select.	Select	Select		
R.08	**Principle/Rule 7** Information can be corrected if requested			Select		Select.	Select	Select		
R.09	**Principle/Rule 8** Information is accurate, relevant etc before use/disclosure			Select		Select.	Select	Select		
R.10	**Principle/Rule 9** Information is not kept longer than necessary	The legal requirements for the retention of transcript data generated by Heidi are not yet fully determined, and formal legal advice will be sought as part of the implementation process. Heidi does not store transcripts indefinitely by default.	Seeking legal advice. Transcript information in summary is still retained elsewhere, such as in the clinical record.	**Medium**	A process for the appropriate transfer, retention, and secure storage of transcript data will need to be developed in alignment with Health NZ policies, legal requirements, and best practice standards for health information management if legal advice suggests this.	**Rare**	**Minimal**	**Low**	CK Jin	30 December 2025
R.11	**Principle/Rule 10** Information is used for the purpose it was collected			Select		Select.	Select	Select		
R.12	**Principle/Rule 11** Disclosure of information			Select		Select.	Select	Select		
R.13	**Principle/Rule 12** Disclosure outside of New Zealand			Select		Select.	Select	Select		
R.14	**Principle/Rule 13** Using/assigning unique identifiers			Select		Select.	Select	Select		
R.15	**AI** Use of AI within the project			Select		Select.	Select	Select		

Target Risk Rating Table

Consequence	Rare	Unlikely	Possible	Likely	Almost Certain
Severe	Medium - 11	High - 16	High - 20	Extreme - 23	Extreme - 25
Major	Medium - 7	Medium - 12	High - 17	High - 21	Extreme - 24
Moderate	Medium - 4	Medium - 8	Medium - 13	High - 18	Extreme - 22
Minor	Low - 2	Medium - 5	Medium - 9	High - 14	High - 19
Minimal	Low - 1 **RO1,**	Low - 3	Medium - 6	Medium - 10	High - 15

Probability

Probability Descriptions:

Rare	Event not occurred and is not expected to occur <5% chance of occurring
Unlikely	Event could occur but may not have occurred before 5-20% chance of occurring
Possible	There is evidence this event has occurred before 21-50% chance of occurring
Likely	Event has occurred several times, likely to occur again in near future 51-91% chance of occurring
Almost Certain	This event is expected to occur imminently >95% chance of occurring

Consequence Descriptions:

Please refer to the Enterprise Risk Management Framework document here (page 18) for specific Domains (i.e. Clinical/Patient Safety), and their associated consequence descriptions. If you are unable to access the framework, it can be provided to you by the National Privacy Office.

Target Risk Rating Calculation:

Low	<80% of risks are GREEN
Medium	50-80% of risks are YELLOW and/or GREEN
High	20-50% of risks are YELLOW, ORANGE and/or RED
Extreme	>20% of risks are allocated as RED
Unknown	Risk table cannot be completed

Appendix 2: Glossary

Please complete the following table with terms, abbreviations, and acronyms you have used in this PIA.

Term	Definition, description, relationship, and business rules
HNZ	Health New Zealand | Te Whatu Ora

Health New Zealand
Te Whatu Ora

CHIEF EXECUTIVE - CONTRACT APPROVAL FORM

NAME OF CONTRACT (and any reference number)	Enterprise Services Agreement – AI Ambient Scribe (ESA) Data Processing Agreement (DPA)
FULL LEGAL NAME OF COUNTERPARTY (including NZBN or equivalent registration number)	Heidi Health Trading Pty Ltd ABN - 84 649 783 871
DESCRIPTION OF CONTRACT	AI Ambient Scribes are a new category of AI technology that capture and summarise clinician–patient conversations into structured clinical notes. Compared with traditional transcription, AI scribes offer real-time documentation, reduce clinician workload, and enable clinicians to focus on patient care. Health NZ has seen rapid organic, fragmented adoption of Heidi solutions across the clinical user community. This agreement will capture and replace all existing Heidi agreements within HNZ. The Enterprise Services Agreement (ESA) and Data Processing Agreement (DPA) between Health NZ and Heidi Health will govern the use of Heidi's AI platform. The ESA sets out a one-year term with renewal options, S9(2)(b)(ii) and strict service, privacy, and security obligations, including ISO27001 and SOC2 compliance, data sovereignty, and no secondary use of Customer Data. The DPA ensures Heidi processes personal information solely on Health NZ's behalf, in line with the Privacy Act 2020, with strict controls over confidentiality, breach reporting, and subcontractor use. Heidi Health has largely adopted the contractual controls recommended by Health NZ's legal and privacy teams. Their service delivery response and restoration targets align with industry expectations, and as a Tier 3 system, Heidi's default delivery standards exceed those of HNZ. However, the absence of service credits and limited consequences for failing to meet critical service levels present some risk. These risks are considered acceptable for an initial deployment. Please refer to the residual commercial points outlined below. See residual commercial points below.
HEALTH NZ CONTACT (Name, Role and Function)	Sonny Taite, Contract Owner, Health X
START DATE	10 October 2026
END DATE	s9(2)(b)(ii)
DURATION (INITIAL TERM)	s9(2)(b)(ii)
RIGHTS OF RENEWAL	s9(2)(b)(ii)
ESTIMATED ANNUAL CONTRACT VALUE	s9(2)(b)(ii)
ESTIMATED TOTAL CONTRACT VALUE	s9(2)(b)(ii)
KEY FINANCIAL DETAILS	Richard Hooper: Endorsed financially noting this is expected to be funded by the s9(2)(b)(ii) Heidi is envisaged in that request at s9(2)(b)(ii) If not approved this will be managed as a Health NZ exposure, s9(2)(b)(ii)
COMPLIANCE WITH GOVERNMENT PROCUREMENT RULES (if applicable)	☒ Yes ☐ No An approved exemption from open advertising has been completed. The exemption is based on rule 14.9.e for the purposes of a Prototype carrying out limited field tests to incorporate findings and in this case to understand technology use cases. The exemption cites the intended future ambient scribe and related technology panel arrangement which would be informed by the operation of this software.
COMPLETION OF CONFLICTS OF INTEREST PROCESSES	☒ Yes ☐ No
DOES THE CONTRACT INVOLVE SHARING OF DATA (if yes, describe protections in place)	☒ Yes ☐ No

	This system has patient data within supplier control for an approved retention period of 14 days where thereafter it will be deleted and non-recoverable except for usage data information used for reporting. The ESA sets out strict service, privacy, and security obligations, including ISO27001 and SOC2 compliance, data sovereignty, and no secondary use of Customer Data. The DPA ensures Heidi processes personal information solely on Health NZ's behalf, in line with the Privacy Act 2020, with strict controls over confidentiality, breach reporting, and subcontractor use.
OTHER NOTES/COMMENTS (including special, unique, or unusual terms and significant risks, impacts, and mitigations)	The following risk profile has been captured and accepted by Health X. Please see the attached Deal on a Page for overall summary of the contractual position.

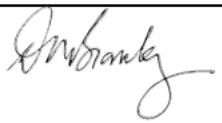
Description	Impact	Mitigation
If there is a 'Material breach', or Termination for Convenience there are no service credits or any pro-rated refund	M	This is for the duration of the initial term or any renewals. s9(2)(b)(ii) .
Subcontractor coverage is light with 'best effort' used as a moderate control of potential Supplier vulnerability	M	
Supplier lock-in	L	Following prototype phase this lock in would be managed via multi-vendor open panel with standard threshold criteria
While the SLAs in the agreement meet the HNZ standard SLA requirements there are no consequences placed on Heidi for unsatisfactory performance (No service level credits)	M	While there are no service credits HNZ retains a Right to Terminate for multiple failures. We have not been able to secure a pro-rata credit of pre-paid subscriptions in this event (i.e. this remains a T4C).
Heidi's unwillingness to take responsibility for any negative impact on their services caused by the non-performance of Heidi's sub-contractors is concerning	H	HNZ has a Right to Terminate for multiple failures.
Heidi doesn't have to notify HNZ of any subcontractors without notice if they meet 6.3 provisions. This does not comply with GCDO Sharing Standard Guidelines	M	HNZ will undertake contract management and regular performance reviews to monitor sub-contractor risks throughout the agreement term.

Attached Documentation	• See Appendix One – Deal on a Page Summary. • Heidi ESA_NZ Final • Heidi DPA_NZ Final • Completed Procurement Recommendation to Endorse & Execute

SIGN-OFF

Each reviewer/approver individually confirms that the contract described in this Contract Approval Form is appropriate for the Chief Executive to approve and sign.

REVIEWER/APPROVER (insert name and role)	SIGN-OFF (signature and date or approval email)
Senior Contract Sign-out Robert Pothan Digital GM Commercial	Contract Approval Form Sign-out Issuer 07/10 - Have reviewed approval documentation and contracts which are in order for execution.
Senior Finance Sign-out Bevan McKenzie Chief Financial Officer	s9(2)(a)

Procurement Sign-out (if relevant) Andy Windsor National Director PSC&HTM	s9(2)(a)
Legal sign-out Andrew Cordner Chief Legal Officer	s9(2)(a)
Digital Services sign-out Darren Douglass Chief Information Technology Officer	s9(2)(a)
Responsible Executive Sonny Taite Health X	s9(2)(a)
CE Approval Dale Bramley Chief Executive	 10/10/2025

Appendix One

Heidi - Enterprise Services Agreement, Ambient Scribe - Deal on a Page Summary

Description	Value
Supplier	Heidi Health Trading Pty Ltd (Heidi)
Deal Name	Enterprise Services Agreement
Target Sign Date	10 October 2025
Deal Summary	
Engagement Type	Ambient AI Subscription for automating clinical documentation.
Contract Type	Heidi ESA (with material edits) AI / SaaS
Duration	Commencement 10 October 2025. s9(2)(b)(ii)
Pricing Type	s9(2)(b)(ii)
Scope – Hardware / Environments	- N/A
Scope – Software	- Heidi AI Ambient Scribe Subscription Licenses - Will capture and replace all existing Heidi agreements within Health NZ - Price per User, per annum, available to all Health NZ entities and districts - Initial volume s9(2)(b)(ii) Users For clarity, Heidi is not the system of record for clinical documentation; Health NZ will retain and manage the system of record copy in accordance with applicable law and policy.
Scope - Services	Onboarding activities, implementation support and ongoing software support.
Security/Privacy	
SRS/PIR Review	Completed in September 2025 – Subject to DPA
Certification	Complies with ISO27001, SOC 2, NZ Privacy Acy 2020 and Health Information Privacy Code 2020

Description	Value
Key Commercials	
Legal Review	Karen Billinghurst (Digital Services)
Transaction	Heidi AI Ambient Scribe s9(2)(b)(ii) s9(2)(b)(ii)
License	Term Subscription for s9(2)(b)(ii) This Agreement is for all regions. Existing agreements to be consolidated within this Agreement.
Warranty	"As Is" warranty only See SLAs for performance targets.
Payment Terms	- Subscription – Annually in advance. s9(2)(b)(ii)
Supplier Indemnity & Liability	- Indemnity and unlimited cap for 3rd Party IP, data breach or security incident, breach of privacy laws, or breach of Confidential Information - Other Liability capped at 1 x 12 month fees.
HNZ Liability	- Capped at s9(2)(b)(ii) - Indemnity and unlimited cap for 3rd Party claims arising out of our use of the platform in breach of the Agreement .
T4C	T4C, 30 Days notice. (No pro-rated refund of Fees paid in advance).
IP	- Platform remains with Heidi - Any Customer Data, prompts and clinical content and paid modifications IP is owned by HNZ.
Penalties / Consequence of Failure ("skin-in')	SLA credits None. Consequences of failure: - Platform unavailable for >24hrs or 3 missed P1, P2 or Availability SLAs in 12 months, HNZ has right to terminate but no Refund of Fees paid in Adv
Roadmap	- None provided
Disengagement	- 60 day disengagement period - secure export of any Customer Data
Deal construct is a s9(2)(b)(ii) ariable SaaS like pricing contract, with right of renewal for subsequent s9(2)(b)(ii)	

Description	Value
Service Model – Clinical critical Tier 3	
Support Scope	- Only includes assistance with issues which are exclusively due to an error with Heidi's Services - Detailed in Specification Documents
Support Model	- 1st Level Support provided by HNZ Service desk - 2nd level support provided from New Zealand by Hendrix. - 3rd level support provided by Heidi - 8 x 5 NZ Business Days

Priority		Deal SLA	Industry Std	% / Credit	HMZ Std
Response Target	P1	30 min	2 Hrs	None	All / 5%
	P2	60 min	4 Hrs		
	P3	12 hrs	24 Hrs	None	-
	P4	24 hrs	48 Hrs	None	-
Restore SLAs Target	P1 Crit	4 hrs	4 hrs	None	All / 7.5%
	P2 Sig	8 hrs	8 hrs	None	90% / 5%
	P3	10 b. Days	10 b Days	None	-
	P4	10 b. Days	1 Mnth	None	-
Availability (Critical)		99.5%	99.5%	None	5%

HNZs Contractual Risks	
No Refunds	No refund of Fees Paid in advance for any Termination (For Breach or Convenience)
No Consequence	No consequence for unsatisfactory performance other than Right to Terminate. (No SL Crs)
No Responsibility	Only best efforts to align Subcontractors to SLAs
Subcontractor Consent	Heidi only has to seek HNZs consent to use a new Subcontractor if they cannot get the new subcontractor to contract to meet the HNZ Contracts SLAs and features or functionalities.

DATA PROCESSING AGREEMENT

This Data Processing Agreement ("Agreement") is entered into between:

(1) Health New Zealand a Crown agent established by section 11 of the Pae Ora (Healthy Futures) Act 2022 (the "Agency"), acting as an Agency as defined under the Privacy Act 2020 (NZ);

AND

(2) Heidi Health Trading Pty Ltd (the "Service Provider"), an entity incorporated in Australia, engaged to process Personal Information strictly on behalf of the Agency,

(together referred to as the "Parties").

WHEREAS:

(A) The Agency is subject to the Privacy Act 2020 (NZ) and determines the purposes and means of processing Personal Information.

(B) The Service Provider provides services to the Agency under the Enterprise Services Agreement entered into on or about the date of this Agreement that involves the processing of Personal Information on behalf of the Agency. The Parties agree that this Agreement forms part of the Enterprise Services Agreement.

(C) The Parties wish to ensure that any such processing under the Enterprise Services Agreement complies with the Privacy Act 2020 (NZ) and other relevant regulatory requirements, and is within the scope of the Service Provider's obligations and responsibilities in the Enterprise Services Agreement;

NOW, THEREFORE, the Parties agree as follows:

1. DEFINITIONS

1.1 In this Agreement, unless the context requires otherwise:
- "Act" means the Privacy Act 2020 (NZ).

- "Agency" has the meaning set out in section 4 of the Act and refers to the Party that determines the purposes for which Personal Information is collected, used, or disclosed.
- "Service Provider" means a person or organisation engaged by the Agency to carry out services involving the handling of Personal Information on behalf of the Agency and solely in accordance with its instructions.
- Enterprise Services Agreement means the agreement between the Service Provider and the Agency for the Agency's use of the Heidi Platform and Services.

"Information Privacy Principles (IPPs)" refers to the privacy principles set out in the Act.
- "Personal Information" has the meaning given in section 7 of the Act, being information about an identifiable individual and in the context of this Agreement relates to Personal Information contained in the Customer Data.
- "Privacy Commissioner" means the Office of the Privacy Commissioner of New Zealand.
- "Subcontractor" means any person engaged by the Service Provider to process Personal Information on behalf of the Agency.

Any terms used in this Agreement, but not defined in this Agreement, have the same meaning as in the Enterprise Services Agreement.

2. NATURE OF PROCESSING

2.1 The Service Provider shall only handle Personal Information on documented instructions from the Agency in accordance with the Enterprise Services Agreement, including in relation to international transfers.

2.2 The Service Provider's role is to process the Personal Information for the Agency. Under section 11 of the Privacy Act 2020, the Service Provider holds the Personal Information for processing on behalf of the Agency. To avoid doubt, the Service Provider may not use the Personal Information for any purpose other than to provide the Services.

2.3 The handling of Personal Information must be strictly limited to what is necessary for the performance of services as agreed between the Parties in the Enterprise Services Agreement.

3. CONFIDENTIALITY

3.1 The Service Provider shall ensure that all persons, including employees, contractors, agents, or Subcontractors, authorised to access or handle Personal Information on behalf of the Agency under the Enterprise Services Agreement are subject to a binding written confidentiality agreement or a statutory duty of confidentiality under applicable law that is consistent with the Service Provider's requirements around confidentiality, privacy, and information security in the Enterprise Services Agreement.

3.2 The Service Provider shall establish and maintain appropriate internal policies, training, and monitoring processes to uphold confidentiality obligations and protect against unauthorised access, use, or disclosure of Personal Information.

3.3 The Service Provider shall promptly notify the Agency of any suspected or actual unauthorised access, use, or disclosure of Personal Information that could constitute a breach of confidentiality, in addition to its obligations around information security and privacy set out in the Enterprise Services Agreement.

4. SECURITY MEASURES

4.1 The Service Provider shall implement and maintain comprehensive technical and organisational security measures appropriate to the level of risk associated with the nature of the Personal Information being handled, including measures to prevent loss, unauthorised access, use, alteration, or disclosure, in line with Information Privacy Principle 5, and consistent with its obligations set out in the Enterprise Services Agreement.

4.2 Such measures shall include, but are not limited to:
(a) access controls and role-based permissions;
(b) secure storage and encryption (at rest and in transit);
(c) vulnerability management and patching;
(d) audit logging and monitoring;
(e) business continuity and disaster recovery planning.

4.3 The Service Provider shall review and update these security measures regularly to ensure ongoing effectiveness and alignment with emerging threats and applicable regulatory requirements.

5. SUBCONTRACTORS

5.1 The Service Provider may engage Subcontractors to assist in delivering the services under this Agreement with the Agency's prior written consent.

5.2The Service Provider must enter into a written agreement with the Subcontractor requiring equivalent data protection obligations consistent with its obligations set out in the Enterprise Services Agreement and this Agreement.

5.3 A current list of approved Subcontractors (also referred to as subprocessors) is set out in the Enterprise Services Agreement..

6. INDIVIDUAL REQUESTS

6.1 The Service Provider shall implement and maintain procedures to identify, track, and report to the Agency any request received from an individual exercising their rights under the Privacy Act 2020, including but not limited to rights of access, correction, and objection.

6.2 The Service Provider shall notify the Agency of any such request within three (3) business days of receipt and provide all information necessary to assist the Agency in responding to the request in accordance with the statutory timeframes.

6.3 The Service Provider shall not respond directly to any request unless explicitly authorised in writing by the Agency. Any such response shall be consistent with the Agency's instructions and the requirements of the Act.

6.4 The Service Provider shall provide reasonable assistance to the Agency in fulfilling such requests, including through appropriate technical and organisational measures to ensure accessibility, traceability, and accountability of Personal Information.

7. PRIVACY BREACHES

7.1 The Service Provider shall implement appropriate policies and procedures to detect, assess, and respond to potential or actual privacy breaches affecting Personal Information, consistent with its obligations under the Privacy Act 2020, and consistent with its obligations set out in the Enterprise Services Agreement

7.2 The Service Provider shall notify the Agency without undue delay and within 24 hours upon becoming aware of a privacy breach that is, or may be, notifiable under the Act.

7.3 The notification shall include, to the extent known:
(a) a description of the breach, including the categories and approximate volume of Personal Information affected;
(b) likely consequences of the breach;
(c) the remedial actions taken or proposed to be taken; and
(d) the name and contact details of the person handling the breach on behalf of the Service Provider.

7.4 The Service Provider shall assist the Agency with any notification to affected individuals or to the Privacy Commissioner, as may be required under the Act.

7.5 The Service Provider shall cooperate fully in any subsequent investigations, audits, or remediation activities and shall retain appropriate records of all privacy breaches and related correspondence.

8. DATA RETENTION AND DELETION

8.1 Upon termination or expiry of the Agreement, the Service Provider shall, at the written direction of the Agency, either return all Personal Information in a structured, commonly used and machine-readable format or securely delete it from all systems, including backups, unless retention is required by law. Service Provider will not store any Personal Information for longer than the period of the Health NZ retention window specified in the Enterprise Services Agreement.

8.2 The Service Provider shall certify in writing to the Agency that such return or deletion has been completed within thirty (30) business days of termination or expiry.

8.3 Where deletion is not feasible due to legal or technical constraints, the Service Provider shall notify the Agency and continue to ensure the confidentiality, integrity, and security of

the retained Personal Information and limit further processing to only that which is strictly required under applicable law.

9. AUDIT RIGHTS

9.1 The Service Provider shall make available to the Agency, upon reasonable notice and during normal business hours, all information necessary to demonstrate that it is handling the Personal Information responsibly, that it is complying with this Agreement and with its obligations under the Privacy Act 2020.

9.2 The Agency shall have the right to view the results of audits no more than once annually unless required for cause or as set out in the Enterprise Services Agreement (e.g., following a data breach).

9.3 The Service Provider shall co-operate fully with any such requests and shall implement any reasonable remedial measures required by the Agency as a result of findings from an audit.

10. INTERNATIONAL DATA TRANSFERS

10.1 The Service Provider shall not transfer Personal Information outside of New Zealand or Australia without prior written consent of the Agency

11. GOVERNING LAW AND JURISDICTION

11.1 This Agreement shall be governed by and construed in accordance with the laws of New Zealand.

11.2 The Parties submit to the exclusive jurisdiction of the courts of New Zealand.

11.3 The Parties acknowledge and agree that this Agreement is valid and legally binding on the Parties.

IN WITNESS WHEREOF, the Parties have executed this Agreement by their authorised signatories:

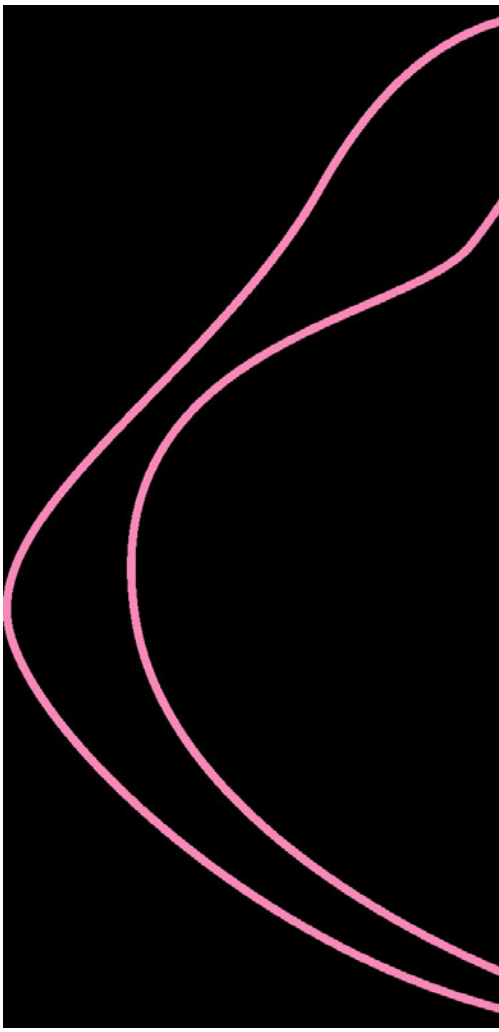
For and on behalf of the Agency:
Signature: _____
Name: Dale Bramley
Title: Chief Executive
Date: 1010/2025

For and on behalf of Heidi Health Trading Pty Ltd:
Signature: _____
Name: Yassin Omar
Title: Head of Legal and Regulatory Affairs
Date: 10/10/2025

heidihealth.com

Organisation Name

Enterprise and Technical Implementation Overview



Contents

Technical Overview

This document provides an overview of Heidi Health's core features and technical safeguards to support cybersecurity assessments by healthcare entities and government departments.

Heidi is an ambient AI scribing platform designed to streamline clinical documentation. It is built with a security-first architecture and includes a number of robust protections to ensure data integrity, confidentiality, and access control throughout its lifecycle

Authentication & Access Controls

Heidi enforces Multi-Factor Authentication (MFA) as a mandatory requirement for all users to ensure secure account access. MFA is performed via a second authentication factor, typically, through an email or SMS code, which must be entered alongside the primary login credentials.

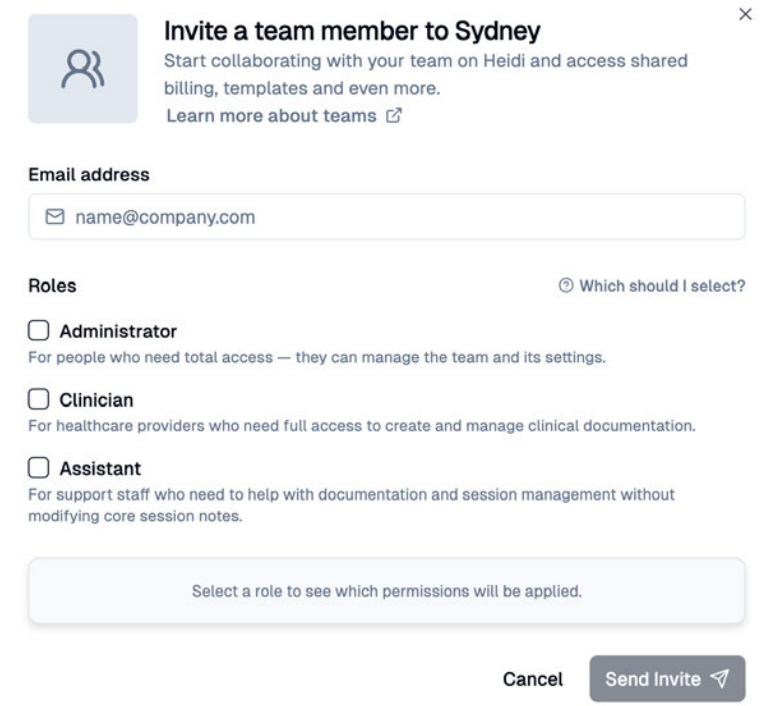
The platform also is at capacity to support integration with enterprise-grade Single Sign-On (SSO) solutions. This allows your organisation to leverage your existing identity and access management infrastructure, providing users with seamless access to Heidi while maintaining centralised oversight and governance over authentication.

Access to platform features is governed by a Role-Based Access Control (RBAC) model. Users are assigned roles—such as Administrator or Clinician and, clinicians and their colleagues are all part of a team specific to the organisation —with permissions scoped accordingly.

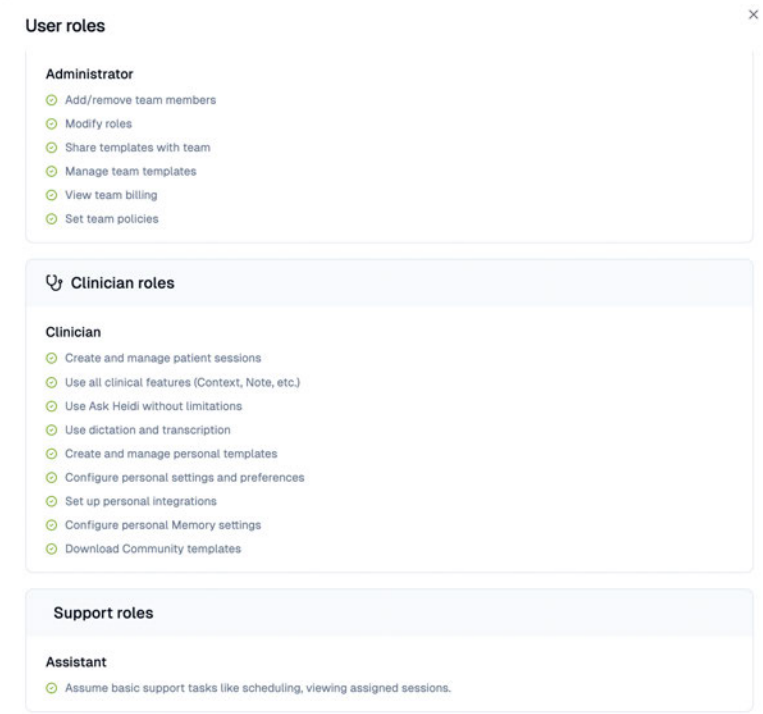
Administrators can configure organisational settings, manage team members, enforce retention policies and edit shared templates. Clinicians have functional access limited to session use, note generation, and personal preferences within the application, ensuring principle of least privilege is upheld.

Typically, the project lead and/or the internal clinical Heidi champion within your organisation will act as the Administrator. More information can be found at https://intercom.help/heidi-health/en/articles/9560724-heidi-teams.

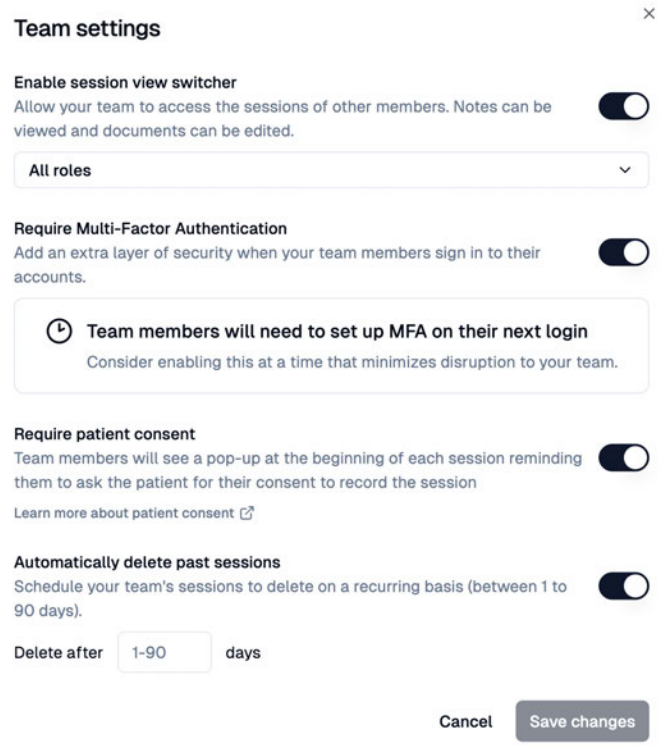
Team Invitation



User Roles



Team Settings



Data Retention & Deletion

Heidi provides administrators with control over data retention via automated lifecycle policies. Admin users can define how long session data are retained within the system (e.g. 7 days is the standard retention period, and available for configuration). Once the retention period expires, Heidi automatically deletes the data in a secure and irreversible manner, ensuring compliance with data minimisation and retention obligations under relevant legislation.

In addition to automation, organisations retain full manual control over their data. Through the Admin interface, users can export, review, and delete records on demand. This flexibility empowers teams to manage health information in accordance with your local recordkeeping policies, audit requirements.

Clinical Note Generation & Template

Heidi's clinical documentation features are powered by AI and underpinned by a structured templating system. Templates define note format, AI instruction parameters,

and content structure—allowing clinicians to generate consistent and high-quality documentation.

Admins have the authority to manage shared templates across the team, ensuring standardisation of clinical language and documentation practices within the organisation. Clinicians can create or edit personal templates, but only Admins can modify templates that apply to the entire team. Templates include section headers (e.g. “Subjective”, “Plan”) and natural language prompts (e.g. “Include family history if mentioned”), which guide the AI in generating appropriate content.

All data processed in a session is done in a secure way, subject to data encryption in transit and at rest, and data pseudonymisation. External materials, such as imaging results or longform PDFs, can be uploaded for context during the session, but are not retained by the platform unless the user manually chooses to include them in a note or save them.

Privacy & Consent Management

Heidi supports privacy safeguards and informed consent practices. Each session can be configured to trigger a consent pop-up by the admin, ensuring that patients are explicitly notified of the use of ambient documentation technology. Verbal consent workflows are also supported and can be standardised across the organisation.

All users operate within a closed team environment, meaning that clinical data, session records, and templates are only accessible to users within the same team. This structure enables internal collaboration while enforcing strict data segregation.

On the backend, Heidi applies logical data isolation for all customers. Each organisation’s data is stored using separate encryption keys. This ensures that no cross-tenant data exposure can occur and supports compliance with jurisdictional health data protection laws, including the New Zealand Health Information Privacy Code.

Logging, Monitoring & Compliance

Heidi logs all user activities to ensure transparency, traceability, and security. This includes login events, session access, administrative actions, and configuration changes. These logs can be provided upon request and Heidi will soon allow such logs to be accessed by authorised Admin users for audit or investigation purposes.

The platform is developed and maintained in alignment with industry-recognised security frameworks, including ISO/IEC 27001:2022 and SOC 2 Type II. In addition to

general compliance with security best practices, Heidi meets region-specific legal requirements under the Australian Privacy Principles (APPs), and especially aligns with the intent of the New Zealand Privacy Act and HIPC framework.

Incident Handling & Support

Heidi maintains formalised incident response procedures to address cybersecurity events, system vulnerabilities, and other safety issues such as hallucinations. Security events are triaged, investigated, and resolved with high priority. In the rare case that a hallucination (AI-generated fabrication) is detected, users are encouraged to report the incident so it can be reviewed and mitigated.

Users can access technical and product support directly via the in-platform help button or by emailing support@heidihealth.com. Escalation procedures are in place for both clinical and cybersecurity matters, allowing rapid involvement of senior support personnel and internal compliance leads.

Implementation Overview

Implementation Overview Summary

The implementation process ensures a seamless rollout of our AI medical scribe, supporting healthcare professionals in reducing administrative burden and enhancing documentation quality. This playbook outlines the plans and processes to ensure a successful deployment across your organisation. It captures each phase of the rollout (Alpha, Beta, and Broad rollout), including best practices, success metrics, implementation timeline, training strategies, support structures, and the escalation protocols that help maintain continuity of care.

Best Practices for a Successful Implementation

- **Engage Early & Often** – Involve key stakeholders from the outset
- **Start Small, Scale Smart** – Begin with a core group, then expand to broader teams
- **Keep It Simple** – Focus on high-impact workflows first

Goals & Success Metrics

Successful implementation of Heidi is guided by clear goals and measurable success metrics that help shape our implementation timeframes and recommendations. These goals ensure that every phase of implementation aligns with organisational priorities and drives meaningful outcomes. Goals may include, but are not limited to, improving documentation quality, reducing administrative workload to save clinicians time, and enhancing overall clinician satisfaction.

To ensure we track success effectively, we leverage a combination of qualitative and quantitative data collection methods. This includes pre-, mid- and post-implementation surveys to assess clinician workload, satisfaction, and documentation efficiency. We also track platform-level usage metrics such as adoption rates, session counts, and the volume of notes and documents generated, amongst many others. By continuously monitoring these indicators, we ensure Heidi is delivering meaningful impact and aligning with the organisation's objectives. We share this data in a transparent manner to ensure alignment on implementation progress and strategy.

A Strategic Approach

To ensure optimal success with large-scale Heidi implementations, we recommend:

Utilising a Phased Rollout Approach

A phased rollout ensures a smooth integration of Heidi into clinical workflows, allowing for iterative improvements and minimising disruptions. By starting with a selected group before expanding, we can:

- Identify and resolve any workflow challenges early
- Gather valuable feedback from initial users to refine processes and personalise training material to allow for a scalable and smooth broad rollout
- Gradually scale adoption across departments, ensuring comprehensive support and engagement

Consider Areas with the Highest Need and Motivation

Implementation is most effective when it begins in departments or teams that are overwhelmed with documentation demands and struggling to keep up with paperwork, as they stand to benefit the most from automation and efficiency improvements. These areas also tend to have a strong willingness to adopt new solutions, and typically:

- Experience high documentation burdens and administrative inefficiencies
- Have clinicians who recognise the value of automation and are eager to engage
- Serve as early adopters who generate momentum, advocating for Heidi's benefits

Focus on Areas That Have Lower Documentation Workflow Complexity First

To ensure a smooth transition, it is beneficial to focus on implementing Heidi in areas with more straightforward documentation workflows. This approach:

- Reduces friction in early adoption by avoiding highly complex, specialised documentation needs
- Allows users to become comfortable with Heidi's core functionality before introducing more advanced use cases
- Helps build confidence and trust in the system, making it easier to expand to more complex areas later.

Note: That being said, it is also recommended to select challenging environments to test Heidi's full capability in the early stages of the rollout. The Emergency Department for example is a popular place to have Heidi tested due its fast paced and frenzied nature.

Implementation Timeline

Our implementation follows a structured approach with clear milestones to ensure smooth adoption and efficiency. We also use exit criteria before progressing to the next phase, ensuring stability without unnecessary complexity.

Note: The size and speed of each phased rollout primarily depend on the number of organisational workflows. For example, a large GP organisation with standardised workflows can onboard a larger cohort and complete a company-wide rollout much faster than a multi-hospital organisation implementing Heidi across diverse departments.

Phase	Key Activities	Exit Criteria
Preparation & Planning	- Align on objectives, governance, and IT requirements - Select sites/departments/users participating in Alpha - Identify workflows and prepare training material	- Organisation objectives are set - IT requirements fulfilled
Alpha Phase	- Provide initial training to selected Alpha users - Heidi team support and follow up during the first few weeks to instil confidence in the Heidi workflow - Post-Alpha phase survey to check in with clinicians - Alpha champions validate the process in preparation for Beta - Further personalisation and finetuning of scalable training material (with the support of Alpha users) - Select sites/departments/users participating in Beta	- Ensure 100% engagement in training - At least 85% activation - Refinement of scalable training material

Beta Phase	- Provide live and asynchronous personalised training to Beta users - Post-Beta phase survey to check in with clinicians - Beta champions validate the process in preparation for broad rollout - Further personalisation and finetuning of scalable training material ahead of the broad rollout	- At least 75% activation - Completion of scalable training material
Broad Rollout	- Full-scale deployment across remaining users. - To optimise long-term adoption, continuous engagement with users, via drop-in office hour sessions and communications, will be maintained. - Regular check-ins with organisational leads will ensure that the implementation remains aligned with the organisation's goals.	- Onboarding completed: 100% of clinicians have access to accounts and training

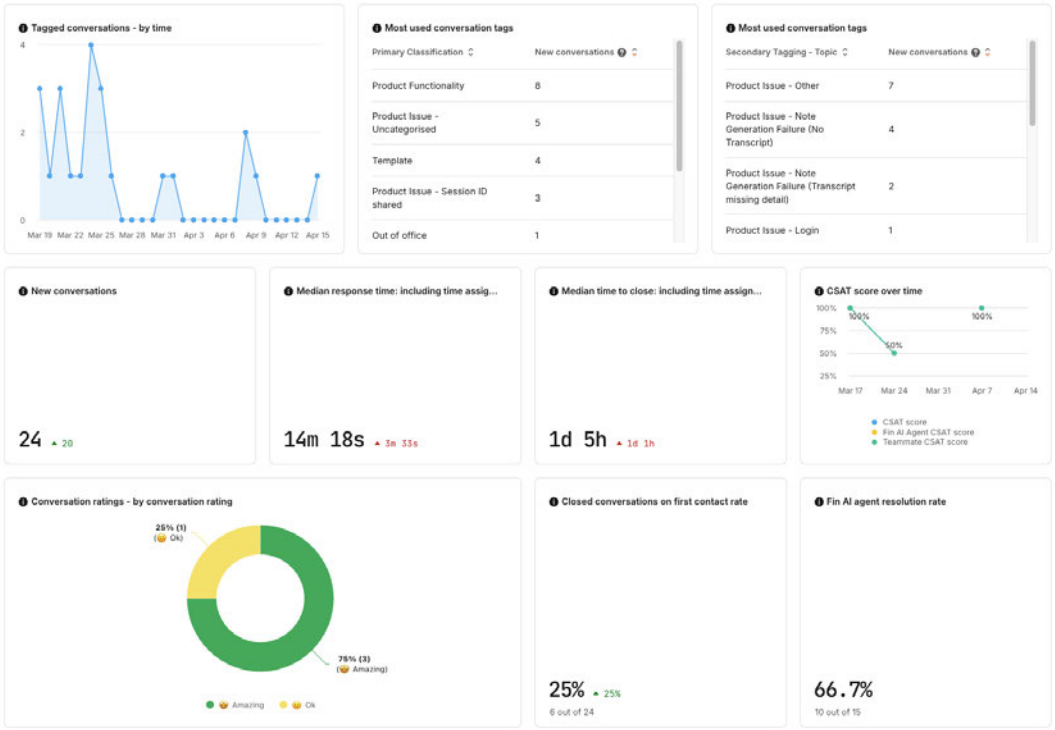
Support Pathways

Ensuring successful adoption requires ongoing support and engagement:

- **Customer Success Team** – Dedicated customer success personnel for project management support, training, troubleshooting, and performance tracking
- **Self-Serve Training Resources** – Access to personalised training materials in order to help create a robust and scalable internal resource center for your organisation. However, to start we do have Heidi Guides, Learning Center articles, and a User Handbook for getting started with Heidi:
    - Heidi Guides
    - Learning Center
    - User Handbook
- **Optional Office Hours** - The Heidi team hosts weekly office hours specific to your organisation throughout the Alpha and Beta phases, whereby clinicians can drop-in and ask product questions, troubleshoot an issue and build templates
- **Regular Check-Ins with Organisation Leads** – Cadence determined on kick-off but typically once a week, at least for the duration of the alpha phase
- **Priority In-Product Support** – Priority support via the Heidi Intercom support channel

We are also able to track and measure user support inquiries for your group that come in via Heidi's support widget and support email (both linked together via Intercom). This combined data is displayed for us within an internal dashboard similar to the below

image and can be tagged categorically, thereby allowing us to tailor our support model and training sessions accordingly, if trends on support needs are identified.



Training Modalities

Training is a combination of **interactive guided learning and self-guided modules**, ensuring flexibility and accessibility for all users. To ensure smooth adoption, we offer role-specific training sessions:

- **Train-the-Trainer Model** – Heidi Champions play a key role in driving adoption, but they are not expected to lead formal training. Instead, we encourage the organisation's project team to assist with just the basic support/ training, ensuring they feel comfortable and equipped to support their colleagues
- **Admin Training** – Focuses on system management, user access, general product features and template customisation
- **End-User Live Training** – Hands-on sessions to familiarise users with Heidi's core functions and discuss how Heidi fits into their workflows
- **Interactive Online Training & Self-Paced Guides** – Optional asynchronous training resources are available for users who prefer flexible learning - we highly recommend that all users review these and have them as reference

Project Management Support

We offer **comprehensive project management support** to assist the organisation's project team throughout implementation. Stated above already, but this includes:

- **Regular Correspondence** – Ongoing communication to ensure alignment and address challenges
- **Interactive Tracking** – Tools to monitor progress and ensure implementation stays on course
- **Heidi Handbook & Documentation** – Comprehensive resources to guide the project team

Customer Success

Our Customer Success team remains actively engaged with your project management team and end users to drive adoption and establish feedback loops. Continuous collaboration ensures that Heidi is optimised for your organisation's needs, with ongoing improvements based on user insights.

- **Direct Communication with Users** – Regular engagement with users via email, training sessions and support channels to reinforce best practices and encourage adoption
- **Continuous Product Updates** – As Heidi evolves, we ensure your organisation takes full advantage of new features and enhancements
- **Feature Voting & Feedback** – We strongly encourage users to provide input on new feature preferences, helping shape the future of Heidi

By following this structured approach, your organisation will maximise the benefits of Heidi Health, ensuring long-term success in reducing administrative burden and enhancing clinician efficiency.

Risk Assessment & Mitigation Strategies

Risk	Risk Level	Mitigation strategy
Low clinician buy-in due to workflow disruption	Low	Pre-testing, efficient and effective onboarding process, strong clinical champion advocacy. Landing page/ Internal organisation page for all clinicians to refer to for resources.
Technical issues affecting Heidi quality	Low	Rigorously tested infrastructure. Prioritised online help support for all participants.

Breakdown in communications between Heidi & Organisational Leads	Low	Support dashboard, weekly check-in meetings, along with regular usage insights provided.

Health New Zealand
Te Whatu Ora

Heidi AI Scribe AI Security Assessment Report

To:	Product Owner Dr Cheng Kai (CK) Jin - Clinical Director | Artificial Intelligence Laboratory, Planning, Funding and Outcomes Business Owner Dr Lara Hopley - Chief Clinical Informatics Officer Security Representative – Syed Hussaini, Kranthi Amaravadi, Fahim Abbasi
From:	Security Consultant – Syed Hussaini
CC:	
Date:	22/10//2025
Subject:	**AI Security Assessment Report for Heidi AI Scribe, SFD#1292**

Purpose

1. This report is the AI security assessment report for the use of Heidi An AI-powered ambient scribing tool used by Te Whatu Ora Clinicians to generate medical notes from recorded consultants.
2. It is intended to provide security risk classification, control gaps, and remediations required to reduce risk exposure for Health New Zealand Te Whatu Ora (HNZ).

Summary

3. Heidi operates as a web-based SaaS platform accessible via browser or mobile devices. Audio is captured from clinical consultations, securely uploaded to Heidi's infrastructure, and then transcribed and summarised using AI models. The final clinical note is available for clinician review and editing. All data is encrypted in transit and at rest, and transcripts can be configured to automatically delete after exporting to the relevant electronic health record.
4. Data is stored and processed in the Australia region. Heidi does not store or retain any patient data beyond the configured retention window, and no data is used to train AI models
5. Generative AI model –Heidi's Generative AI model might not be resident in the NZ/AU approved region
6. The information stored/processed in the system is classified as Medical In-Confidence
7. The privacy assessment is completed
8. Triage Summary

Item	Details
Vendor	Heidi AI Scribe
Use Case	Heidi is a digital health platform that provides real-time clinical

Health New Zealand
Te Whatu Ora

	documentation support to clinicians using AI-driven voice transcription and summarisation. It is designed to reduce the administrative burden on healthcare providers by generating accurate, human-readable medical notes from consultation audio
Deployment Type	Vendor hosted SaaS
Autonomy Level	Low
PHI processed	Yes
Clinical Impact	Yes

Health New Zealand
Te Whatu Ora

Security Control Status

The table below shows security control gaps identified in this system.

Control ID	Control Title	Status	Findings / Gaps
GOV.01 – AI System Registration	**Register Heidi in AI System Register.**	Met	Added to Cyber AI System Register
GOV.02-Accountable Owner Designation	**Assign accountable owner.**	Met	Added to Cyber AI system Register
GOV.03-Documented Purpose & Alignment	**Document purpose & scope Provide system security overview and evidence of governance processes**	Met	Added to Cyber AI System Register. Heidi provided ISO 270001 certificate, and it is valid until May 2026 SOC 2 Type 2 report is also shared.
GOV.05-Risk Acceptance by Governance Body	**Governance body accepts PHI/Clinical risk.**	Met	NAAIEG approved (June 2025)
DIP.07-Purpose Limitation & Minimization	**Complete Privacy engagement to review Data Handling and Privacy Impact.**	Met	Privacy Assessment Completed
DIP.05-Encryption of Data in Transit & at Rest	**Enforce encryption in transit/rest.**	Met	All data is encrypted in transit using TLS 1.2+ and at rest using AES-256 encryption, including for backups and across both primary and secondary storage locations. All application traffic occurs over HTTPS.
DIP.06-Data Classification & Sensitivity Tagging	**Confirm data residency.**	Met	For New Zealand users, all data is hosted in secure AWS servers located in Australia
DIP.09-Third-Party Data Handling Controls	**Provide contracts with PHI handling clauses.**	Met	As per Enterprise Service Agreement with Health NZ

Health New Zealand
Te Whatu Ora

DIP.10-Data Retention & Disposal	**Share disposal processes.**	N/A	Audio recordings in the system contains PHI. Data is securely and irreversibly deleted using secure data erasure methods in compliance with applicable privacy and data protection laws. However, Heidi is not a system of record, Outputs from the system are copied to the system of records (PMS, EHR, EMR). Clinicians can delete the recordings from the Heidi Platform
IAM.02-Authentication & Session Control	**Integrate Heidi with enterprise SSO.**	Not Met	HNZ SSO needs to be enabled as part of this implementation – due date TBC
IAM.01-Role-Based Access Enforcement	**Define RBAC roles, review and revoke access quarterly.**	Not Met	HNZ SSO needs to be enabled as part of this implementation – due date TBC
IAM.02-Authentication & Session Control	**Provide MFA capability and secure session controls.**	Not Met	HNZ SSO needs to be enabled as part of this implementation – due date TBC
IAM.04-Logging of Access Events	**Provide audit logs for access.**	Met	Heidi maintains audit logs for user access, system changes, data access, and security events, including authentication attempts, changes to user permissions, and access to sensitive data. Logs are retained for a minimum of one year to comply with regulatory and operational requirements, with critical security incident logs retained for extended periods as needed. Logs are reviewed regularly by compliance and security teams, with automated tools assisting in analysis and alerting of suspicious activities. Audit logs are available upon request.
IAM.05-Review and Revocation of Access	**Access to AI systems must be reviewed quarterly, with immediate revocation for inactive or offboarded users.**	Not Met	HNZ SSO needs to be enabled as part of this implementation – due date TBC

Health New Zealand
Te Whatu Ora

SUP.01-AI Vendor Due Diligence	**Provide ISO 27001/SOC 2 certification.**	Met	ISO 270001 certificate provided, and it is valid until May 2026 SOC 2 Type 2 report is also shared.
SUP.01-AI Vendor Due Diligence	**Supply penetration test reports.**	Met	Penetration Test report supplied by Vendor Dated 17th Feb 2025
SUP.03-Provenance & Version Tracking	**Provide provenance/version history.**	Not Met	Unable to confirm where this model resides, no clarity provided by the vendor.
INP.01-Input Type & Format Validation	**Define and provide accepted input formats (audio/file standards).**	Met	['.wav', '.mp3', '.mp4', '.aac', '.flac', '.ogg', '.webm']
INP.02-Input Length & Complexity Bounds	**Demonstrate schema validation, token guardrails.**	Met	Schema Validation - All API endpoints enforce JSON Content-Type and strict request/response schemas - Server-side validation rejects unknown/extra fields, enforces types/ranges, and caps payload size; malformed payloads return 4xx with error codes. - Layered protections: rate limiting and AWS WAF managed rules (SQLi/XSS/command injection) at the edge; app-layer validation at the service. Token guardrails - Authentication uses signed JWTs; every request is checked for signature, issuer/audience, exp/iat and token revocation on logout. - We implement automatic session disconnection on inactivity that is configurable - All auth traffic is over TLS 1.2+; token storage follows least-privilege/Http only where applicable
INP.04-File and Attachment Handling	**Show file handling controls.**	Met	WAF policies allow only listed file types with size limits and header inspection. Audio is processed in real-time chunks and transmitted directly for transcription without persistent storage, minimising data retention risk.
ETH.02-Transparency of Delegation Boundaries	**Ensure clinical staff are trained on explanation support.**	Partial Met	Ensure clinical staff are trained on explanation support and escalation workflow for inaccurate and harmful responses.

Health New Zealand
Te Whatu Ora

MON.02-Output Logging with Input Reference	**Retain input/output logs.**	Met	Heidi retains the logs for at least 1 year
MON.03-Access-Controlled Log Retention	**Provide log retention controls.**	Met	Heidi retains the logs for at least 1 year
MON.04-Model Output Risk Monitoring	**Implement output monitoring.**	Met	Heidi retains the logs for at least 1 year
IR.05-Stakeholder Notification Plan	**Define clinical escalation workflow.**	Partial Met	Have a training program available for HNZ clinical staff.
IR.01-AI Output Incident Thresholds IR.02-Escalation and Containment Procedures	**Share incident thresholds and containment procedures.**	Met	Incident Response Plan categorizes incidents by severity (S1-Critical, S2-High, S3/S4-Low/Medium) with defined escalation protocols and response timelines. All incidents documented in Service Log with critical incidents undergoing root cause analysis https://app.aus.vanta.com/c/heidihealth.com.au/doc/policy/incident-response-plan-bsi/en
IR.05-Stakeholder Notification Plan	**Notify Health NZ of incidents per SLA.**	Met	Incident notifications provided per SLA terms in the ESA.
RSL.03-Fallback Mode or Manual Escalation	**Define fallback workflow if vendor unavailable.**	Not Met	BCP to be discussed and have a training program available for HNZ clinical staff
RSL.02-Availability Targets for AI Services	**Share availability targets.**	Met	All incidents can be accessed via https://status.heidihealth.com 99%
RSL.05-Redundancy and Failover Mechanism	**Provide redundancy/failover documentation.**	Met	Heidi's redundancy strategies including AWS multi-AZ deployments, and automated failover procedures. Remote work activation and redundant communication channels ensure service continuity
RSL.06-Resilience Testing & Incident Simulation	**Provide results of resilience/DR testing.**	Met	Disaster recovery testing conducted quarterly per Business Continuity Policy with documented results of failover procedures, data restoration, and service recovery times.

Health New Zealand
Te Whatu Ora

ETH.03-Ethical Impact Assessment for AI Use	**Complete Ethical Impact Assessment** **Ensure governance body reviews ethical risks.**	Met	As approved by NAAIEG (June 2025)
ETH.02-Transparency of Delegation Boundaries	**Provide disclaimers and transparency features.**	Met	In-product warnings require clinicians to verify all AI-generated content before use. Patient information sheets and consent forms available via Resource Centre. Our Usage Policy clearly state clinician responsibility for final documentation. Platform includes explicit disclaimers about AI limitations and probabilistic nature.

Health New Zealand
Te Whatu Ora

Key Risks & Residual Exposure

The table below shows current security risks identified in this system.

Risk	Consequence	Likelihood	Risk Rating	Comments
Unowned or Unregistered AI	Major	Unlikely	Medium (14)	
Excessive or Unsafe Data Handling	Major	Unlikely	Medium (14)	
Weak Access Controls	Major	Possible	High (18)	This risk will be re-assessed after implementing SSO with HNZ entra ID
Vendor and Supply Chain Blind spots	Major	Possible	High (18)	Unable to confirm where this model resides, no clarity provided by Heidi
Poor Input Handling and Exposure	Major	Unlikely	Medium (14)	
Insufficient Monitoring or Logging	Major	Unlikely	Medium (14)	
Uncontained Failure or Drift	Major	Unlikely	Medium (14)	
Model Overreach or Misbehaviour	Major	Possible	High (18)	Unable to confirm where this model resides, no clarity provided by Heidi
Unreviewed or Biased Decisions	Major	Unlikely	Medium (14)	
Inadequate Response and Recovery	Major	Unlikely	Medium (14)	

Health New Zealand
Te Whatu Ora

Recommended Remediations

The table below describes the security controls that are necessary to reduce security risk exposure, so that it falls within the risk appetite. All actions are owned by the Product Owner/Business Owner.

Control ID	Action Required	Priority Order (1,2,3)	Due Date
IAM.01-Role-Based Access Enforcement	Integrate Heidi with HNZ enterprise SSO and reassess	1	TBC
IAM.05-Review and Revocation of Access	Define RBAC (Role based access control) with RBAC roles to be reviewed ad revoke access quarterly.	1	TBC
SUP.03-Provenance & Version Tracking	Unable to confirm where this model resides, no clarity provided by the vendor.	1	Feb 2026
ETH.02-Transparency of Delegation Boundaries	Ensure clinical staff are trained on explanation support and escalation workflow for inaccurate and harmful responses.	2	Feb 2026
IR.05-Stakeholder Notification Plan	Have a training program available for HNZ clinical staff	2	Feb 2026
RSL.03-Fallback Mode or Manual Escalation	BCP to be discussed, Have a training program available for HNZ clinical staff	2	Feb 2026

Health New Zealand
Te Whatu Ora

Health New Zealand
Te Whatu Ora

1.	Note:	The current risk of the solution is **High**	Noted
3	Note:	The Product Owner and Business Owner are responsible for completion of the remediations recommended in this report.	Noted
4	Risk Acceptance	We accept the risks and recommendations described in this memo.	Yes

Signature_____ Date:

Dr Cheng Kai (CK) Jin - Clinical Director | Artificial Intelligence Laboratory ,Planning, Funding and Outcomes

(as **Product Owner**)

Signature_____ Date:

Dr Lara Hopley - Chief Clinical Informatics Officer

(as **Business Owner**)

Signature_____ Date:

Peter Booth – Chief Information Security Officer (Acting) - Health New Zealand

Health New Zealand
Te Whatu Ora

Appendix 1 – Risk Matrix

Likelihood	Consequence: Minimal	Minor	Moderate	Major	Severe
Almost Certain	Medium (8)	High (15)	High (17)	Extreme (23)	Extreme (25)
Likely	Medium (7)	Medium (10)	High (16)	High (19)	Extreme (24)
Possible	Low (3)	Medium (9)	Medium (12)	High (18)	High (22)
Unlikely	Low (2)	Low (5)	Medium (11)	Medium (14)	High (21)
Rare	Low (1)	Low (4)	Low (6)	Medium (13)	High (20)

Appendix 2 – Likelihood Table

Likelihood	Probability of occurrence	Qualitative description
Almost Certain	>90%	Regularly happens / expected to occur in most circumstances.
Likely	61-90%	Has happened / probably will occur in most circumstances.
Possible	31-60%	Might occur in some circumstances/has happened occasionally.
Unlikely	10-30%	Not expected but could occur in some circumstances/has happened infrequently.
Rare	<10%	May occur in specific or exceptional circumstances / no known history.

Health New Zealand
Te Whatu Ora

Appendix 3 – Consequence Table

	MINIMAL	MINOR	MODERATE	MAJOR	SEVERE
Goals and objectives	Slight deviation from our critical priority KPIs and strategic objectives.	Shortfall in meeting our critical priority KPIs and strategic objectives.	Noticeable shortfall in meeting our critical priority KPIs and strategic objectives.	Significant challenges in achieving our critical priority KPIs and strategic objectives, affecting our operational efficiency and strategic direction.	Failure to meet our critical priority KPIs and strategic objectives, jeopardising our strategic initiatives and overall organisational success.
Health Outcomes	Isolated instances of errors, delays, or misdiagnoses that do not result in serious harm but in minor adjustments in protocols and minimal consumer concern.	Isolated incidents of errors, delays, or misdiagnoses resulting in adverse effects for some consumers, prompting internal reviews and minor corrective actions.	Notable increase in errors, delays, or misdiagnoses resulting in adverse effects for a group of consumers prompting investigations and corrective measures.	Widespread breakdown of health systems, resulting in serious harm to consumer groups and urgent investigations.	Critical health systems failures, resulting in numerous deaths or permanent harm among consumers.
	Minimal impact on short-term, or likelihood of long-term, population health outcomes. Minimal delay (<6 months) in Determinants of Health (DoH) activities.	Some impact on short-term, or likelihood of long-term, population health outcomes. Time-limited impact on usual public health activities. Minor delay in progress on DoH activities >6 months.	Moderate impact on short-term, and/or likelihood of long-term, population health outcomes. Extended impact on usual public health activities. Moderate delay in progress on DoH activities >1 year.	Major impact on short-term and likelihood of long-term population health outcomes. Major, +/- sustained impact on usual public health activities. Significant delay in progress on DoH activities >3 year.	Significant impact on short-term population health with likelihood of adverse impact on long-term population health. Severe, sustained impact on usual public health activities. Failure to progress on DoH activities.
	Barriers to access result in minimal disruption for certain population groups. Impacted population groups experience minimal delays and inconveniences in accessing suitable and timely care.	Barriers to access result in minor disparities in health outcomes for certain population groups. Impacted population groups frequently experience delayed first presentation to the health system.	Barriers to access result in moderate disparities in health outcomes for certain population groups. Impacted population groups experience late and/or multiple presentations on entry to the health system.	Barriers to access result in widespread disparities in health outcomes for certain population groups. Impacted population groups experience more serious diagnoses.	Barriers to access result in profound and systemic disparities in health outcomes, Impacted population groups experience premature loss of life.
Our people	Work-related mental or physical harm not requiring any intervention or treatment.[1]	Work-related physical harm requiring first aid treatment but no lost time. Mental harm requiring peer support.	Work-related mental or physical harm or ill health requiring treatment by a registered health professional. Restricted work/alternate duties/lost time of <7 days.	Work-related mental or physical harm leading to a WorkSafe notifiable event and injury/ illness. Work-related harm resulting in permanent disability or chronic physical or mental health condition/lost time of > 7 days.	Work-related fatality or multiple fatalities. Work-related harm resulting in multiple cases of permanent disability or chronic health conditions.
	Manageable challenges in aligning people, culture, and capability with no impact on productivity, retention, and morale.	Misalignments in people, culture, and capability with a minor impact on productivity, retention, and morale.	Noticeable misalignments in people, culture, and capability impacting overall productivity organisational effectiveness, employee engagement, retention, and morale.	Major misalignments in people, culture, and capability impacting team dynamics, productivity, and organisational performance, retention, and morale.	Severe disruption in people, culture, and capability severely impacting productivity, retention, and morale.
Service Disruption	Disruption with a minimal single service or district/local impact to health delivery. (Caused by e.g. clinical equipment, infrastructure, suppliers, supply chains, and technology).	Disruption with a minor single service or district/local impact to health delivery. (Caused by e.g. clinical equipment, infrastructure, suppliers, supply chains, and technology).	Disruption with a moderate multi-district/multi-local or regional impact on health delivery. (Caused by e.g. clinical equipment, infrastructure, suppliers, supply chains, and technology).	Disruption with major multi-region or national service impact on health delivery. (Caused by e.g. clinical equipment, infrastructure, suppliers, supply chains, and technology).	Disruption with a severe national impact on health delivery. (Caused by e.g. clinical equipment, infrastructure, suppliers, supply chains, and technology).
Legal and Regulatory	One-off compliance issue with no chance of prosecution or financial penalty (e.g. Breach of Code of Rights or privacy resulting in ex-gratia payment <$20k). Local negligence or breach of a district/local level contract resulting in a low-value civil claim, financial settlement, or judgement (<$50k). No impact on Certification/Accreditation status.	Repeated minor compliance issues with minor chance of prosecution with minor financial penalties (e.g. Breach of Code of Rights or privacy resulting in ex-gratia payment <$50k). Negligence or breach of a district/local level contract resulting in a civil claim, financial settlement, or judgement value ($50k - $100k). No impact on Certification/Accreditation status.	Compliance issues with potential for prosecution and/or moderate financial penalties (e.g. Breach of Code of Rights or privacy resulting in ex-gratia payment >$50k). Negligence or breach of a district/local or regional level contract resulting in a civil claim, financial settlement, or judgement value ($100k - $1m). Local changes needed to ensure Certification/Accreditation status is not affected.	Compliance issues with major prosecution/litigation and/or financial penalties. Negligence or breach of a regional or national level contract resulting in a civil claim, financial settlement, or judgement value ($1m - $5m). Certification/Accreditation status may be affected, or conditions imposed.	Compliance issues with severe prosecution/litigation and/or financial penalties. Material negligence or breach of a regional or national level contract that may result in a civil claim, financial settlement, or judgement value (>$5m). Systemic changes needed to ensure the health system achieves compliance.
Perception and Reputation	Isolated complaint without media attention. Limited potential for public concern.	Local media coverage resulting in short periods of public confidence loss. Elements of public expectation not met.	Moderate sustained adverse media attention. Limited short-term impact on public confidence.	Major adverse media event/coverage. Prolonged loss of public trust and confidence. Chief Executive/Ministerial intervention.	Severe sustained adverse media event/coverage. Complete loss of public trust and confidence. Parliamentary enquiry/intervention.
Finance Opex budget Capex budget	Up to 0.10% unfavourable variance to Opex budget. <2% unfavourable variance to Capex budget.	>0.10% up to 0.15% unfavourable variance to Opex budget. 2% to <5% unfavourable variance to Capex budget.	>0.15% up to 0.20% unfavourable variance to Opex budget. 5% to <7.5% unfavourable variance to Capex budget.	>0.20% up to 0.25% unfavourable variance to Opex budget. 7.5% to <10% unfavourable variance to Capex budget.	>0.25% unfavourable variance to Opex budget. 10% and greater unfavourable variance to Capex budget.
Programme and Project Delivery	Minimal delays or disruption (internal/external), contained within tolerances and with little to no impact on Delivery, Output(s), Outcome(s), Benefit(s), and/or BAU.[2]	Delays or disruption (internal/external) that could be contained within existing tolerances and/or managed within approved contingencies, with a possible impact on Delivery, Output(s), Outcome(s), Benefit(s), and/or BAU.	Delays or disruption (internal/external) that will exceed existing tolerances and contingencies, resulting in a direct impact on Delivery, Output(s), Outcome(s), Benefit(s), and/or BAU.	Major delays or disruption (internal/external) that will exceed existing tolerances and contingencies, requiring a formal change request to mitigate/remediate the risk(s) to failure of the project and/or programme.	Severe events resulting in total failure of the project and/or programme.

Risk Management Process.pdf