

Indici AI: Privacy Impact Assessment Report

28 JANUARY 2025

Contents

Project summary 2

Scope of the PIA 2

 Scope 2

 The process 2

Personal information 3

Privacy assessment 4

Risk management 7

 R-001: Patient consent 7

 R-002: Accuracy of generated medical notes 7

Recommendations to minimise impact on privacy 8

Action plan 9

References 10

Project summary

Indici CoPilot is an additional set of AI tools developed by Valentia Technologies integrated into the Indici practice management system (PMS), including but not limited to the ability to transcribe GP consultations. This is achieved by capturing an audio recording of a medical consultation between a practitioner and a patient, using a combination of speech-to-text transcription and large language models (LLMs) to produce either a summary or structured medical note. This output can then be exported directly into a patient's medical records.

This privacy impact assessment (PIA) seeks to investigate the potential privacy risks of implementing Indici AI in this form from the perspective of Pinnacle, on behalf of its member practices.

Scope of the PIA

Scope

This project covers the implementation of Valentia Technologies' "Indici AI" tool within member practices of Pinnacle Midlands Health Network, when used as an integrated part of the practice's practice management system (PMS). This PIA covers:

- what additional information may be collected by Indici AI as part of its use in patient consultations;
- how Indici AI may capture, store, and process the information it collects from the patient and practitioner.

Issues considered to be out of scope for this PIA include:

- existing procedures and processes around the storage of patient notes within the PMS;
- additional features of Indici AI unrelated to consultations.

The process

This PIA was completed by Pinnacle's Privacy Officer and members of the Data Team, based on private correspondence with Valentia Technologies from December 2024.

Personal information

The process of transcribing and summarizing a consultation by Indici AI follows the data flow outlined below.

1. Before the beginning of the consultation, the practitioner downloads the “IndiciTranscriber” app on their phone from the App Store, allowing them to record consultations directly on their phone. A QR code on the patient’s file allows the recording to be uploaded to Indici at the end of the consultation. Alternatively, recordings can be done through the PC microphone.
2. During this medical consultation, a wide range of personal information may be provided by the patient about themselves, much of which may be particularly sensitive.
3. After the conclusion of the consultation, the practitioner uploads the recorded audio to Indici. If recorded on the practitioner’s phone, this can be done using a QR code on the patient’s file.
4. This audio is then transcribed by an audio transcription service hosted internally by Indici.
5. The transcript is then processed to mask personal information (via AWS Comprehend), then summarized by either:
 - a. a LLM hosted externally by a third-party (e.g., Azure ChatGPT, OpenAI ChatGPT, Claude Sonnet) which has been determined by Valentia to not store submitted data or use it for training purposes;
 - b. a LLM hosted internally by Indici.
6. The returned summary can then be edited by the practitioner before saving it to the patient’s record in Indici.

Valentia has indicated that the audio recording of the consultation is not stored on their servers, but the transcription may be saved indefinitely as part of the patient’s record.

Privacy assessment

This section outlines the principles set out in the Privacy Act, which form the legal framework that Pinnacle needs to consider when deciding to implement Indici AI in practices.

Each row in the following table summarises the key requirements of each of the privacy principles, and outlines how the implementation of Indici AI may impact each principle. Based on this summary, Indici AI has been assessed as being compliant or non-compliant with each principle, with any additional information linked to a numbered risk.

#	Description of the privacy principle	Summary of personal information involved, use and process to manage	Assessment of compliance
1	Principle 1 - Purpose of the collection of personal information Only collect personal information if you really need it.	Patient data is collected for the purpose of summarising consultations into medical notes. Unnecessary data may be collected as part of the recording if brought up by either the patient or practitioner during the consultation, but may be edited out of the medical notes by the practitioner after the completion of the consultation.	<i>Compliant</i>
2	Principle 2 – Source of personal information Get it directly from the people concerned wherever possible.	Indici AI uses only patient data collected directly from the patient during consultation.	<i>Compliant</i>
3	Principle 3 – Collection of information from subject Tell them what information you are collecting, what you're going to do with it, whether it's voluntary, and the consequences if they don't provide it.	To comply with this principle, patients must be aware of and have consented to the recording and processing of their medical consultation by a third-party. Valentia Technologies has indicated that a checkbox is provided as part of Indici AI for GPs to confirm that they've obtained patient consent for recording.	<i>Potentially non-compliant (R-001)</i>
4	Principle 4 – Manner of collection of personal information Be fair and not overly intrusive in how you collect the information.	Indici AI is a non-intrusive ambient AI assistant, which should result in no change to the way in which information is collected during a consultation.	<i>Compliant</i>

#	Description of the privacy principle	Summary of personal information involved, use and process to manage	Assessment of compliance
5	Principle 5 – Storage and security of personal information Take care of it once you've got it and protect it against loss, unauthorised access, use, modification or disclosure and other misuse.	Valentia Technologies states that they store transcripts and structured medical notes if patient consent has been received, storing them on their systems as part of the patient's PMS record. Valentia Technologies have also indicated that they take measures to avoid sharing personally identifying information with third parties by masking it from consultation transcripts and only using third-party LLM providers that do not store submitted data or use it for training purposes.	<i>Compliant</i>
6	Principle 6 – Access to personal information People can see their personal information if they want to.	Implementation of Indici AI would not result in any change to this principle; existing procedures around access to a patient's own notes and medical record would apply, which are out of scope of this PIA.	<i>Compliant</i>
7	Principle 7 – Correction of personal information They can correct it if it's wrong, or have a statement of correction attached.	Implementation of Indici AI would not result in any change to this principle; existing procedures around corrections to a patient's own notes and medical record would apply, which are out of scope of this PIA.	<i>Compliant</i>
8	Principle 8 – Accuracy etc. of personal information to be checked before use Make sure personal information is correct, relevant and up to date before you use it.	The AI models used by Indici AI to summarize a consultation may have biases that affect the accuracy or comprehensiveness of the notes. Inaccurate or incomplete notes could lead to clinical errors or misjudgements, potentially impacting patient care. In order to minimize this risk, practitioners should ensure that they thoroughly review generated medical notes to ensure that the information in them is correct, complete, and unbiased.	<i>Potentially non-compliant (R-002)</i>
9	Principle 9 – Not to keep personal information for longer than necessary Get rid of it once you're done with it.	Valentia Technologies states that they store transcripts and structured medical notes if patient consent has been received, storing them on their systems as part of the patient's PMS record. Storage of these structured medical notes within the patient's PMS record is out of scope for this PIA.	<i>Compliant</i>

#	Description of the privacy principle	Summary of personal information involved, use and process to manage	Assessment of compliance
10	Principle 10 – Limits on use of personal information Use it for the purpose you collected it for, unless one of the exceptions applies.	Indici AI uses patient information provided during the consultation for generating medical notes, which falls under the original purpose of collecting that information.	<i>Compliant</i>
11	Principle 11 – Limits on disclosure of personal information Only disclose it if you've got a good reason, unless one of the exceptions applies.	Implementing Indici AI would result in disclosing patient information to Valentia Technologies for the purpose of them transcribing the consultation and generating medical notes, which is directly related to the purpose for which the information was obtained (11 (1)(a)).	<i>Compliant</i>
12	Principle 12 – Disclosure of personal information outside New Zealand Only send it to someone overseas if the information will be adequately protected.	While Indici AI and the tools it uses to process patient consultations are hosted on global cloud platforms, the Office of the Privacy Commissioner has stated that using "[u]sing offshore technology providers to store or process your data is not treated as a disclosure under IPP12, so long as they are not using that information for their own purposes" [1]. Valentia Technologies have also indicated that they take measures to avoid sharing personally identifying information with third parties by masking it from consultation transcripts and only using third-party LLM providers that do not store submitted data or use it for training purposes.	<i>Compliant</i>
13	Principle 13 – Unique identifiers Only assign unique identifiers where permitted.	Implementing Indici AI would not result in the creation of new unique identifiers for patients.	<i>Compliant</i>

Risk management

Three primary sources of potential risk were identified above:

- patient consent
- accuracy of generated medical notes.

These risks are further detailed below.

R-001: Patient consent

Information privacy principle 3 states in part that if an agency collects personal information about a person, the agency must take any reasonable steps to ensure that the individual is aware of what information is collected, the purpose of that information, and the consequences if that information isn't provided.

As AI transcription of Indici AI's nature is a new and emerging technology, it's especially important that patients are fully informed of its use and how it may impact on their privacy. Failure to do so may result in patient dissatisfaction, ethical issues, or privacy complaints.

Several methods could be used to ensure that patients are aware that Indici AI is being used to record and summarize their consult:

- Seeking explicit consent before activating Indici AI. Valentia Technologies notes that a checkbox is provided as part of the tool for GPs to confirm they've obtained patient consent for recording; it may be beneficial to provide a recommended disclaimer that could be used by GPs at the beginning of a consultation in which they intend to use Indici AI.
- Signage informing the patient that Indici AI or similar tools may be used during a consultation, as well providing a way to find out more information.

R-002: Accuracy of generated medical notes

Information privacy principle 8 states that agencies that hold an individual's personal information must not use or disclose that information with taking reasonable steps to ensure that the information is accurate, up to date, complete, relevant, and not misleading.

It is possible for generative AI tools, including summarisation tools like Indici AI, to produce confident errors of fact and logic ("hallucinations"). Additionally, depending on the training data used, AI model may have inherent biases that could affect the accuracy or comprehensiveness of the notes.

Any issues with the generated medical notes caused by hallucinations or inherent biases, if not identified and corrected, could result in clinical errors or misjudgements, potentially impacting patient care. As such, steps should be taken when using these tools to ensure that the practitioner carefully evaluates the generated data to ensure correctness and accuracy before entering it into the patient's record.

Recommendations to minimise impact on privacy

Summarise the recommendations to minimise the impact on privacy based on your risk assessment.

Ref	Recommendation	Agreed Y/N
R-001	Ensure that patients are made aware of, and consent to, the use of Indici AI in their consultations.	
R-002	Ensure that practitioners review medical notes generated by Indici AI for accuracy and potential bias.	

Action plan

This section of the report should describe what actions are being taken (whether short or long term) and how they'll be monitored. There may also be links to other processes in the organisation. For example, a proposed action might relate to security controls (such as restricting access to a system). This will then link in with security processes in the organisation.

Reporting on the outcome of the mitigation may be necessary. If the PIA is being performed as part of a project, then the project is likely to require some reporting on their implementation as part of governance arrangements. Once the project is completed, any on-going privacy monitoring should be incorporated into normal business operations.

In the case of a particularly long or complex programme of work, the PIA may need to be reviewed a number of times to ensure that it continues to be relevant. This section should describe how this will be achieved.

Ref	Agreed action	Who is responsible	Completion date
R-001			

References

- [1] Office of the Privacy Commissioner, “Artificial intelligence and the Information Privacy Principles,” September 2023. [Online]. Available: <https://www.privacy.org.nz/assets/New-order/Resources-/Publications/Guidance-resources/AI-Guidance-Resources-/AI-and-the-Information-Privacy-Principles.pdf>. [Accessed 11 November 2024].