**Data Protection Impact Assessment:**

**CLINITALK**

To adopt this DPIA for your organisation review the information provided in table 2 and then add your details to table 1 in the yellow boxes.

**Table 1**: Organisation details

|  |
| --- |
| Your details |
| **Your Name** |  |
| **Your Role** |  |
| **Your Email** |  |
| **Your Organisation Name** |  |
| **Date of adoption** |  |

**Box 2**: Data processing impact assessment

|  |  |  |
| --- | --- | --- |
| **Question** | **Response** | **Guidance** |
| **System name** | CLINITALK |  |
| **Data Controller** | The data controller is the organisation named in Box 1  | This is the ‘owner’ of the data that will be processed  |
| **Data Processor** | Clinitalk Ltd | The data processor |
| **Purposes of System/Process** | Overall Purpose: Educational feedback for GP training.Description: Doctors in training record a consultation on the secure Clinitalk web page. After the consultation is complete, they receive immediate feedback. Doctors can link to their trainer to enable joint review of feedback and progress. Benefit: Patients benefit from the additional training received by their doctors and the improved consulting skills that result. The organisation benefits from the additional training support.Data Collected:Consultation audio User registration data: (GMC number, email, ethnicity, prior exam attempts, country of graduation, sex.)Data required to process payments.Purpose of the data collection:Clinitalk collects demographic information about the user to tailor feedback to the user and to create a user account.Data Processing* Consultation audio which may include personal and special category information is collected via a secure web page.
* Data is protected throughout processing and storage by encryption.
* The basis for processing is explicit patient consent.
* Recording data is deleted within 21 days of recording.
* Users can delete recording data earlier.
* Data is stored and processed in compliance with the requirements of the UK-General Data Protection Regulations (UK-GDPR) and the Data Protection Act (2018).
* Data is processed by Clinitalk and its sub processor for the purpose of transcription. As part of the processing names and dates are redacted from the transcript.
* The sub processor holds data for the minimum time necessary to complete transcription typically 1-60 seconds per request. No audio or transcript data is stored by the subprocessor.
* An anonymised transcript (names, and dates removed) is further processed by Clinitalk and its sub processor to generate feedback.

  | This needs to be a description of what the project or process will involve. Explain broadly what the project/processing aims to achieve, what the benefits will be to patients, the organisation, to individuals and to other parties. Is the data to be collected to be used only for a specified purpose – e.g., to provide healthcare, facilitate payment for activities, improve services, clinical audit?       |
| **What Legal bases are to be used to process any data collected?** | Explicit consent (UK GDPR Regulations article 6 and 9).In compliance with UK Regulation and best practice Clinitalk’ s terms and conditions require a doctor in training to request explicit patient consent prior to recording consultation audio. Consent is documented within the application.Post consultation the user interface presents the doctor in training with a question asking them to confirm consent has been obtained. The legal bases for use of the CLINITALK consultation analysis solution by General Practitioner doctor in trainings and trainers:GDPR Article 6, part a – ConsentGDPR Article 9 (2) (h), condition a – Explicit Consent, andSchedule 1 condition 2. the assessment of an employee’s working capacity | Where there will be processing of any personal information, a GDPR Article 6 Legal basis will need to be identified; for any processing of special category information, a GDPR Article 9 legal basis will need to be identified.    |
| **Which Data Subject Rights apply to this/these legal basis/bases and how will these be met?** | * Right to Information
* Right to Access (with potential redaction)
* Right to Rectification
* Right to Object
* Right to object to Automated Processing
* Right to Data Portability

Clinitalk ltd as the data controller will act as the contact point for data subjects and customers requiring assistance in responding to queries about access and individual rights. All enquiries to external data processors should be redirected to Clinitalk Ltd. Note Clinitalk cannot access the encrypted recordings and transcripts it stores. Only the user who generated the recording has the encryption key to access the audio. **Access Request Workflow** 1. Clinitalk receives a data subject access request.
	1. Clinitalk makes relevant identity checks to ensure the request is from a legitimate source.
		1. We request information necessary to respond to the query: the recording’s date, time, location, and the doctor’s name.
	2. Clinitalk supports the data subject by
		1. Explaining that access to a recording is limited to the doctor and their trainer, that encryption prevents Clinitalk from accessing recordings and that all recordings are deleted within 21 days.
		2. Directing them to the relevant customer. The relevant customer holds the encryption key and can identify if a recording exists or has been deleted.
2. Clinitalk informs the customer
	1. Clinitalk messages the customer using the email address provided regarding the data subject request. We inform them of their duty to respond and include the information provided regarding the recording’s date, time, location, and the doctor’s name.
	2. The customer identifies if the audio recording occurred in the last 21 days
		1. If yes – the customer views the data stored and responds to the data subject request. If a deletion request is made the Clinitalk user shall delete the recording and transcript.
		2. If no – the customer informs the data subject that no recordings exist (all recordings and transcripts are deleted 21 days after creation).

As a data processor and controller, Clinitalk ltd will assist healthcare organisations to meet all relevant data subject rights and will inform customers should any request be made by a data subject directly to Clinitalk ltd. Note To help locate a recording in response to a data subject request, users can use the recording date and time stamp. | Data Subject Rights Available: Right to InformationRight to AccessRight to RectificationRight to Withdraw ConsentRight to ObjectRight to object to Automated ProcessingRight to be ForgottenRight to Data Portability (not all rights are applicable in healthcare settings but all opportunities to prioritise the rights and wishes of the data subject with regard to the processing of their data should be considered) |
| **In which locations does the processing take place and who is impacted by the processing?** | Data processed by Clinitalk is encrypted at rest and in transit. Clinitalk processes and stores the following data sets for 21 days following a consultation. 1. Consultation audio, 2: Redacted consultation transcripts.Processing Locations:* Processor location and storage: Microsoft azure data centre South in the United kingdom, United Kingdom
* Sub processor legal basis for processing: GDPR regulation binding contract clauses supervised under UK law.
* The sub processor holds data transiently (typically < 60 secs and not more than 300 secs), processing data at the time of demand and may not store or retain the processed data. Upon completion of processing Clinitalk data, the sub processor will immediately and irretrievably delete the processed data.
* Sub processor location: Assembly AI Ireland.
* Further information: The sub processor has signed the GDPR required legally binding contract clauses. All data is processed under UK law jurisdiction. In particular, the sub processor agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.
* Open AI API a second sub processor is used to process anonymised data and as such is not provided with data containing patient identifiable information such as name, date of birth, dates or addresses. The OpenAI data sharing agreement incorporates the standard GDPR regulation binding contract clauses supervised under UK law. All data is processed under UK law jurisdiction. OpenAI processing is based in Ireland and the US. Clinitalk has requested data to be processed in Ireland.

Clinitalk staff working to support the Clinitalk solution are based in the UK.The processing positively impacts GP surgeries by supporting the GP trainer in providing educational content to the doctor in training to improve their consultation skills.The processing has the potential to positively impact patients by supporting education of the doctor in training towards consulting behaviours that result in improved patient health outcomes.  | Where is the data to be processed?This will include any manual processing and any electronic processing. (Processing includes but is not limited to: any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction) Please list locations for each aspect of processing identified. If the data is to be processed outside the UK, describe the mechanisms and security in place to safeguard the data? Has any data transfer outside the UK been flagged and approved by the Data Protection Officer for the company? |
| **Describe the context of the processing** | Clinitalk is committed to supporting GP trainers and doctors in training to discharge their educational responsibilities safely and securely, including but not limited to the recording and reviewing of consultations to facilitate learning. Clinitalk does not control which consultations are recorded or how long they are stored, other than by limiting storage to no more than 21 days. The doctor in training working on behalf of the practice controls which consultations they record, and when to delete recorded consultations (up to a limit of 21 days storage).Clinitalk terms and conditions requires. * all consultations to be recorded with the consent of the data subject and in accordance with UK regulation.
* users to delete recorded consultations on patient request and to comply with all UK regulation regarding rights, processing, and storage of data.

Clinitalk uses established and proven industry standard encryption and anti-interception technology consistent with that used by other organisations involved in the recording of patient consultations e.g., educational software, cloud telephony.Clinitalk has robust operational processes to ensure that functions carried out by Clinitalk are aligned to UK legislation. For example, change management process compliance checks. Clinitalk has sought the opinion of patients regarding the acceptability of the solution and received support for its use as a training tool in General Practice. The Clinitalk solution has been developed as a digital solution by Clinitalk Ltd to be fully compliant with [NHS Digital information governance and data protection standards.](https://digital.nhs.uk/cyber-and-data-security/guidance-and-assurance/data-security-and-protection-toolkit-assessment-guides)There are currently no security flaws identified in the technology used to provide this solution. | What is the nature of the relationship between the organisation and the data subject?How much control will the data subject have over the processing?Would they expect their data to be used in this way?Do the data subjects include children or other vulnerable groups?Have there been any prior concerns over this type of processing, or security flaws?Is the processing novel in any way?What is the current state of technology in this area if appropriate?Are there any current issues of public concern that you should factor in?  |
| **What personal data will be processed?** | Doctor in training Information including* GMC number, email, ethnicity, prior exam attempts, country of graduation, sex.

Patient Information* With the consent of the patient and doctor in training, Clinitalk stores recorded consultation audio, which may contain patient personal data including but not limited to, name, age, gender, address, health condition. Clinitalk does not have access to the personal data content held within the encrypted consultation.
 | Personal Data means *forename, surname, date of birth, age, gender, address, postcode, NHS Number, another identifier racial or ethnic origin, physical or mental health condition* Please list which Personal Data will be processed. |
| **What Special Category data will be processed** | At the instruction of the user and with the consent of the patient and doctor in training, Clinitalk stores recorded consultation audio in encrypted format, which may contain patient personal data including but not limited to:* Physical/mental health condition diagnoses and conditions
* Symptoms.
* Operations and medical procedures.
* Medications and prescriptions issued.
* Allergies and reactions to medication.
* Results of investigations such as blood tests and X-rays
* Test results.
* Details of services received.
* Details of lifestyle and social circumstances.
* Details of nationality, race and/or ethnicity.
* Details of religion.
* Details of genetic data or biometric data.
* Data concerning sex life and/or sexual orientation.

 Clinitalk does not have the key to access the personal data content held within the encrypted consultation. Only the user who generated the recording has the encryption key. | Special Category data means *personal data related to the physical or mental health of a natural person, including the provision of healthcare services, which reveal information about a person’s health status or any data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation*  |
| **Are individuals explicitly informed about why their personal data is being collected and how it may be used?** | The CLINITALK consultation analysis solution requires data subjects to be fully informed about consultation recording and how it may be used. Users must respect the data subject’s (patient’s) privacy and dignity, and their right to make or participate in decisions that affect them. Users must not make or participate in the making of recordings against patient wishes or where a recording may cause the patient harm. Clinitalk provides users with resources to help them update their [privacy notice](https://www.clinitalk.co.uk/privacy-notice) to inform data subjects about;* **Purpose**: - the training and oversight of doctors to improve patient care
* **Contact details:** info@clinitalk.co.uk
* **Type of data collected:** health information
* **Data source:** Consultation audio recording
* **Lawful basis for collection**: - Patient consent
* **Data sharing**:- Clinitalk does not share patient data with other organisations.
* **Choice**: - It is your choice whether your consultation is recorded.
* **Security**: All consultations are securely stored to prevent against unauthorised access or interception. We use AES256 encryption, one of the strongest security technologies available.
* **Deletion**: Recordings are stored for up to 21 days and deleted on request.

Clinitalk’s privacy notice can be found at clinitalk.co.uk/privacy-notice  | If data collection/processing standards and procedure are not transparent, controllers/data subjects may not trust the processing organisation and refrain from sharing their personal data. Notification should be via a Privacy Notice and may also be via correspondence, leaflets and verbal communication.https://ico.org.uk/for-organisations/sme-web-hub/how-to-write-a-privacy-notice-and-what-goes-in-it/  |
| **What is the process for deleting the data?** | Stored encrypted audio recordings are automatically deleted after a period of 21 days.Users can delete a recording on demand at any point prior to automatic deletion by selecting the recording and choosing the deletion option. Deletion occurs at the time of request.Users can request deletion of their personally identifiable information by contacting info@clinitalk.co.uk. Upon receiving a deletion request Clinitalk will process the request and remove the personally identifiable information. As per the registration terms and conditions, Clinitalk retains anonymised data about the consultations recorded e.g. number of consultations that have been recorded, and speaker interaction statistics such as the time the user spoke during sections of the consultation, for the purpose of recognising patterns of performance, which are used to improve the user experience and educational content provided.Clinitalk holds no access to the encrypted patient data stored, and data subjects contacting Clinitalk regarding an access request will be directed to the relevant user. | Is it necessary to keep all of the data that is being processed? Are there procedures for reviewing how long data should be retained? Is there a policy, procedure, rationale for archiving personal information?  |
| **Describe the information workflow** | A request for information regarding data held by Clinitalk may be received by a healthcare organisation on or behalf of a patient, or it may be a data subject access request (DSAR) from the patient themselves. A DSAR is a specific legal instrument under the data protection legislation and (together with formal evidence of patient consent where this applies) may range in scope from a limited and specified data set to a broader request for information stored. **Access Request Workflow** 1. Clinitalk receives a data subject access request.
	1. Clinitalk makes relevant identity checks to ensure the request is from a legitimate source.
		1. We request information necessary to respond to the query: the recording’s date, time, location, and the doctor’s name.
	2. Clinitalk supports the data subject by
		1. Explaining that access to a recording is limited to the doctor and their trainer, that encryption prevents Clinitalk from accessing recordings and that all recordings are deleted within 21 days.
		2. Directing them to the relevant customer. The relevant customer holds the encryption key and can identify if a recording exists or has been deleted.
2. Clinitalk informs the customer
	1. Clinitalk messages the customer using the email address provided regarding the data subject request. We inform them of their duty to respond and include the information provided regarding the recording’s date, time, location, and the doctor’s name.
	2. The customer identifies if the audio recording occurred in the last 21 days
		1. If yes – the customer views the data stored and responds to the data subject request. If a deletion request is made the Clinitalk user shall delete the recording and transcript.
		2. If no – the customer informs the data subject that no recordings exist (all recordings and transcripts are deleted 21 days after creation).

**Providing information about who has access to consultation audio.**If information is requested about who has access to the consultation audio the healthcare provider should inform the requester that:* Within Clinitalk the Clinitalk user who made the consultation recording has access to the consultation audio recorded in the last 21 days.
* A Clinitalk user can allow their trainer to access recordings stored on their account by linking to their account to their trainer’s account. Therefore, it the Clinitalk user has linked to their trainer, the trainer also has access to the consultation audio recorded in the last 21 days. A doctor in training is not permitted to link to another doctor in trainings account. A doctor in training can only be linked to one trainer account. If the trainer allocated to the doctor in training changes, the linked trainer account can be switched to the new trainer.
* The accounts that have access to a subjects consultation audio can be provided by the doctor in training, or by Clinitalk on request.

  | The collection, use and deletion of personal data should be described, and it may also be useful to refer to a flow diagram or another way of explaining data flows. How will this information be added to the high-level data flow capture process for this area? You should also say how many individuals are likely to be affected by the project. |
| **Will the personal information be shared with or disclosed to other organisations?** | Clinitalk will not disclose patient identifiable data (from the consultation recording or transcript) collected in the course of this processing to any other entity outside the sub processor, the patient themselves, the Clinitalk user who made the recording, and the Clinitalk users clinical trainer. Clinitalk uses GDPR compliant sub processors and has a written contract in place to ensure that Clinitalk data is processed and held securely in line with GDPR requirements and best practice. The agreement states the respective responsibilities of the data controller and processor / sub processor * Sub processor legal basis for processing: GDPR regulation binding contract clauses supervised under UK law.
* The audio sub processor holds data transiently (typically < 60 secs and not more than 300 secs), processing data at the time of demand and may not store or retain the processed data. Upon completion of processing Clinitalk data, the sub processor will immediately and irretrievably delete the processed data.
* Sub processor location: Assembly AI - Ireland
* Further information: The sub processor has signed the UK GDPR required legally binding standard contract clauses that submit itself to the jurisdiction and cooperation with the competent supervisory authority in any procedures required for ensuring compliance with GDPR. In particular, the sub processor agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken. The processor is externally monitored for GDPR compliance and has AIPCA SOC 2 compliance certification.

OpenAI sub processing: OpenAI is used to sub process anonymised data and as such is not provided with data containing patient identifiable information such as name, date of birth, dates or addresses. The OpenAI data sharing agreement incorporates the standard GDPR regulation binding contract clauses supervised under UK law. OpenAI processing is based in Ireland and the US. Clinitalk has requested data to be processed in Ireland. Model training:In accordance with our sub processor agreements, sub processors do not train their models on data provided by Clinitalk.Data transmission and storage:Data is transmitted and stored in an encrypted format to protect against interception and misuse. Storage occurs in the United Kingdom on the secure Microsoft Azure data centre servers situated in UK South. The data centre provider has no ability to read the data at any time. The data centres are staffed 24 hours a day every day of the year, with strict access control, extensive CCTV coverage, and online firewall protection. In the terms and conditions, the user must request obtain patient consent prior to audio recording audio and confirmation of consent must be captured both in the recording and via a probity statement made after recording. The recording will not be processed or stored if the probity statement is not affirmed.Aggregated anonymised user data (e.g. number of consultations recorded, time spent using Clinitalk) is used to analyse system performance, improve user experience, and to encourage user uptake and may be shared with other organisations. We do not share personal information. | Have the other organisation(s) provided written assurances that they will safeguard the information and not share it further? If they do share it with any sub-processors, where does this happen? How will the information be shared? Does the other organisation have an adequate Data Protection Policy compliant with the GDPR? Does the other organisation complete aDSP Toolkit, have Cyber Essentials Plus or ISO27001 compliance? Is there a Contract/SLA or Confidentiality agreement in place?  The contact must clearly state the respective responsibilities of both the Data Controller and Data Processor.If Consent is the legal basis identified for the processing, how/when will this be sought/captured/retained? If promotional videos, brochures or press stories have been developed, has any personal information been anonymised so that even if it were linked to other data, it would not be possible to identify the person? |
| **What are the risks to the data subject?** | There is a risk to the data subject that a consultation recording is accessed unlawfully. Consultation recording for educational purposes is an established process and unlawful access is a risk common to all types of consultation recording processes. Unlawful access may occur through the doctor in training sharing their account log in credentials. To mitigate against this risk users are advised on account creation about lawful access and are required to agree to strict terms and conditions of use including use of complex password credentials and multi factor authentication. To further mitigate the risk of unauthorised access, users may not link their account to another doctor in training account and can only link to a single trainer account. Doctor in trainings must confirm that the trainer account being linked to is the clinical trainer in charge of their clinical supervision.There is a residual risk to data subjects resulting from external penetration of the data centre and the data held on systems. Security provisions are in place to mitigate such a risk, such that any patient identifiable data attacked will be encrypted during all transit and storage thereby being made inaccessible to attackers. Individuals can request their personal data be deleted at any point after a recording has been made.We minimise the period of data storage to that necessary for the intended purpose to limit the storage of sensitive data.  | Explain what practical steps you will take to ensure that you identify and address privacy risks both now and in the future. Who should be consulted, internally and externally? Are individuals provided with the possibility to access and correct their personal information?   Can they request the deletion of some or all of their personal information where this is appropriate to the legal basis being used? Is it necessary to restrict access to data? If so, are these restrictions adequately defined and explained? |
| **What technological and organisational security measures will be put in place to protect the data subject and their rights?** | All patient identifiable data processed is secured in transit and at rest using HTTPS and TLS and AES256 encryption methods to UK legal and NHS standards. Sub processors must complete processing at the time of receipt and may not store or retain data.The data centre storage provider has no ability to read the data at any time. The data centres are staffed 24 hours a day every day of the year, with strict access control, extensive CCTV coverage, and online firewall protection.Clinitalk has Information Governance and Data Security policies in place, and these are regularly reviewed to maintain compliance with regulatory and statutory legislation and guidance.  The organisation completes an annual Data Security and Protection review against the 10 national data guardian standards for data security as per NHS Digital (data security toolkit). Clinitalk has completed the UK Cyber Essentials Plus review by an IASME certified organisation.All Clinitalk staff are trained on their responsibilities for maintaining the proper governance and protection of Information at Induction and annually and are required to maintain familiarity with all relevant Information Governance and Data Security policies and protocols during their employment (Ref: 1018 Asset register and Audits)Additionally, staff working on the development side follow a Standard Operation Procedure (SOP) which will determine actions required to deliver development and supports compliance with data protection legislation at all points in the delivery process.Clinitalk has an Access Control Policy and Acceptable Use Policy in place to ensure that Clinitalk staff access to critical data systems is monitored, and any anomalies flagged immediately to the Senior Management Team.  | What measures are in place to protect access to data (e.g. username/password, role-based access, NHS Smartcard, Secure Access Tokens)Are staff trained/reminded regularly to follow all security and governance policies and protocols when accessing data? Is annual training provided to all staff on good data protection and information security practices? If relevant, is NHSmail used or are e-mails encrypted?   If so, what kind of encryption is used? Are there appropriate anti-virus and anti-malware solutions in place? Does the organisation have DSPT/CyberEssentials accreditation in place? |
| **Is the data regularly backed up and recoverable in the event of a failure?** | Data processed as part of the service is backed up daily providing the capability to restore the service in the event of corruption or data loss. We store this back up on a cloud service. This is an on-line, real-time backup of the entire service and as such no traditional backup media exists.The backups are held for 7 days after which the oldest backups are overwritten. All backed up data stored is compressed, de-duplicated and encrypted to the level of AES 256 bit within a secure vault.Business continuity and disaster recover for the Microsoft azure data centre is provided by the Microsoft datacentre crisis management plan. | Assurances must be made that data is properly backed up and restored at regularly intervals, whether the system is standalone or networked. |
| **What happens in the event of a data breach or loss of data?** | Clinitalk has a robust Security Incident Management Policy in place which defines the scope of potential security incidents (both internal and external) that may affect data processed as part of the Clinitalk service, together with actions to be taken by relevant personnel to both secure the data at the earliest opportunity and to inform relevant stakeholders (data controllers/the ICO/NHS Digital/patients themselves) of any suspected or actual data breach in line with current data protection legislation and all contractual obligations.Clinitalk’s staff supporting the service are required to raise concerns in an open and proactive manner to ensure that potential breaches may be avoided by speedy and pre-emptive action by the company. Our target is to report breeches within 4 hours of discovery to the necessary stakeholders is within 4 hours of discovery. | What action will be taken if there is a data breach?  Is there a requirement at contract level that any data processors inform the organisation at the earliest stage of a suspected or actual data breach? Have you considered some worst-case scenarios regarding what might happen if the personal data collected by your organisation was compromised or deleted either by accident or purposely? Are individuals informed if their personal data is lost, stolen or other compromised?   Will any other organisations need to be informed? |
| **Consultation Process** | Clinitalk has sought the views and discussed the use of consultation recording with patients, doctor in trainings and trainers and the educational team within the Royal College of GPs. We sought patient views within patient clinics and recorded their feedback. We sought doctor in training views using a questionnaire in the initial pilot and from ad hoc responses. We sought trainer views during our trainer education sessions and from ad hoc feedback.We have had overwhelmingly positive responses from our patients and doctor in trainings and educationalists who appreciate the potential benefits for care and education and the need for a tool that can scale to meet the countries growing needs. We will continue to seek the views of our stakeholders as we develop Clinitalk to improve the experience and address concerns. We will do so in the form of stakeholder questionnaires and in response ad hoc contacts we receive. | Describe when and how the views of relevant individuals will be/have been sought (or describe why this is not appropriate).Who else within the organisation needs to be involved?Do you need assistance from any sub-processors?Do you need to consult/have you consulted any information security experts or other experts? |
| **Summary of the DPIA Outcomes** | The Clinitalk service covered by this DPIA is assessed as being a robust and secure method for Clinitalk to support GPs to carry out necessary functions for the maintenance and improvement of GP education.Clinitalk is responding to an identified need for educational support and only records doctor in training and patient data based on explicit consent.The existing security measures in the Clinitalk product, together with the internal procedural controls of Clinitalk will further embed the principles of data protection by default and design in the Service.  Additionally, the escalation and oversight architecture of the Clinitalk Service, includes a Data Protection Support Officer to give further assurance that data subject rights are central to the processing carried out as part of the Clinitalk Service. The DPSO will be responsible for ensuring that any risks to data are quickly identified and mitigated by the protocols to be established for the secure running of the Service.Privacy concerns shall be reported to and investigated by the DPSOThe Clinitalk program, with its data processing activities, has various impacts on privacy, security, and other relevant considerations. By implementing appropriate measures to address the identified impacts, such as ensuring privacy compliance, securing data during transmission and storage, and maintaining data accuracy and transparency in analysis, Clinitalk can mitigate potential risks and provide a valuable tool for improving doctors' consultation skills while safeguarding patient data. Regular monitoring, auditing, and updating of the DPIA will help ensure ongoing compliance and effectiveness of the program. | List the key DPIA outcomes: Have you identified all risks and mitigating actions above?  Who is responsible for integrating these outcomes back into the project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved?    Who is the contact for any privacy concerns which may arise in the future? |

|  |  |  |  |
| --- | --- | --- | --- |
| **Outstanding Risks to Clinitalk** | **Outstanding Risks to Data Subjects** | **Mitigations in Place** | **Residual Risk** |
| **None outstanding** | **None outstanding** |  |  |
|  |  |  |  |

|  |
| --- |
| **Clinitalk Risk Assessment Completed By:** |
| **Name** | **Dr Nicholas Boeckx FRCGP, MRCP, MBChB** |
| **Role** | **Director / Head of compliance** |
| **Date** | **16/01/2025** |
| **Version Number** | **1** |
| **Processing Entered onto Record of Processing Activities?** | **Yes** |
| **Outstanding Risks Entered into Risk Register?** | **No outstanding risks** |

|  |
| --- |
| **Agreed by Director** |
| **Comments/Issues identified** | **None** |
| **Name** | **Peter Salmon** |
| **Date** | **16/01/2025** |
| **Date of next review** | **January 2027 – or sooner if processing activity changes out of scope of this DPIA** |