Health and care:
Template data protection impact assessment (DPIA)

Background

A data protection impact assessment (DPIA) will help you to identify and mitigate potential data protection risks to an acceptable level before using or sharing (processing) data that identifies individuals (personal data).

A DPIA will also help you meet a number of data protection legal requirements including:

- Data protection by design - privacy and data protection issues must be considered at the start, or in the design phase, of a new system, product or process, then continuously while it exists.
- Accountability - your organisation is responsible for showing how it complies with data protection laws.
- Transparency - personal data must be used and shared in a transparent way.
- Security - adequate measures need to be in place to protect data. This can range from policies and procedures to technical security measures such as encryption of data.

DPIAs are mandatory when there is a high risk to individuals, such as when using the health and care data of a large number of people. However, health and care organisations are strongly advised to complete a DPIA when using and sharing personal data in a new or substantially changed way.

A DPIA involves a risk assessment. If a high-level risk remains after applying mitigations, then you must consult with the Information Commissioner's Office (ICO) for further advice before starting to collect, use or share the data.

A DPIA is a live document - you must update it if there are any changes to:

- the purpose - why you are proposing to use or share personal data
- the manner - how you will use or share the data
- who is involved - the organisations using and sharing personal data

This is a template DPIA for health and care organisations to use when rolling out an AI-enabled scribing tool to support individual care. We encourage organisations to adopt it. The template is written so that it is easy to use without needing expertise in data protection. It is the responsibility of the organisation which is deciding on why and how the data is being used and shared (known as the controller), to ensure that the DPIA is completed appropriately.

If you are intending to use an AI-enabled scribing tool for other purposes, such as for supporting internal meetings where only staff data is discussed or for supporting research you will need to complete a separate DPIA.

Additionally, if you are using data that was originally collected as part of providing individual care for any further purpose, such as for research, training the tool or any other use, will require separate consideration, and has not been included in this DPIA. In relation to research purposes, please see the Health Research Authority's DPIA guidance.

Text in [square brackets and green highlight] is guidance only and should be removed for the final version.

Text in yellow highlight is sample wording and should be edited according to your local circumstances.
Text in blue has been added by X-on Health.

Table of contents

Data protection impact assessment (DPIA)

Data protection impact assessment (DPIA) title:	AI-enabled ambient scribing tool Surgery Intellect, powered by TORTUS

SECTION 1 – Screening questions

1. **Do you need to do a DPIA?**

We consider that the implementation of this tool requires a DPIA because:

- It is a new technology and therefore we will use the DPIA to identify potential risks and implement measures to protect personal data and ensure compliance with data protection laws.
- As the use of AI is not widely understood and may be considered high risk, the DPIA will assist to foster greater confidence and trust in the AI technology.
- It is possible that the tool will process a large amount of personal data and special categories of personal data, therefore a DPIA will help to ensure that this data processing is compliant and safe.
- AI scribe outputs will create new personal data about individuals, therefore a DPIA will help to ensure that this information is managed appropriately.
- Processing special category health data, involving AI summarisation, and relying on cloud infrastructure, they meet the ICO's criteria for mandatory DPIA.
- [add any others]

a. **Summary of how data will be used and shared**

AI-enabled ambient scribing products, also known as ambient scribes or AI scribes, are a type of AI tool that listen to and record conversations and turn these into a task-specific output, such as a summary or a letter.

- Ambient and Telephone Consultations: The system listens to and transcribes both in-person (ambient) and telephone consultations via the X-on Phonebar.
- Clinical Documentation: It generates accurate patient consultation notes, letters, and referral letters, reducing the cognitive load for clinicians.
- Clinical System Integration: Once reviewed and approved by a clinician, the generated content is filed directly into the patient record within the core clinical system (e.g., EMIS Web, TPP SystmOne, OneAdvanced Vision) and synced back to Surgery Connects patient contact history.
- Decisions about care will only be made by health and care professionals. They may use AI scribes to assist them, but will review all suggestions made by an AI scribe and will never rely on an AI scribe alone to make decisions about care.

Decisions about care will only be made by health and care professionals. They may use AI scribes to assist them, but will review all suggestions made by an AI scribe and will never rely on an AI scribe alone to make decisions about care.

[Note that this DPIA only covers the use of these tools to support individual care. It does not cover any other use such as for supporting research, training AIs, or internal use of staff data. You will need to complete a separate DPIA for these uses]

b. Description of the data

☒	Personal data (name, DOB, contact details)
☒	Special category data (Medical information from Ambient and call consultations)
☒	Technical metadata (IP address, browser environment) and call metadata (time stamps)

SECTION 2 – Why do you need the data?

2. What are the purposes for using or sharing the data?

The purpose of using the data is to allow the tool to fulfil the following tasks, which will contribute to the aim of reducing administrative burden on health and care professionals and assist them in providing care to individuals:

Input information functions:
- capture/record speech interactions
- capture/record phone call interactions
- incorporate other secondary information, provided directly by the user or otherwise, for example, extra context or external information from health records.

Output information functions:
- convert speech interaction recordings into text transcripts
- generate summaries based on text transcripts. These can be driven and structured according to templates, which can sometimes be customised
- format outputs according to a particular style or structure
- extract and link terms to clinical codes
- generate outputs in the form of medical letters or other documentation
- populate information in health records
- suggest actions or other tasks like scheduling or referrals

3. What are the benefits of using or sharing the data?

Reduces administrative burden
The purpose of the tool is to reduce administrative burden, freeing up health and care staff to focus their time on other specialist tasks, for example providing individual care. This may also contribute to improved job satisfaction and overall well-being of staff.

Enhances accuracy and completeness of documentation
The aim of the tool is to improve the quality and completeness of documentation by reducing errors in transcription, ensuring that no critical details are missed, and standardising the documentation process.

Supports data-driven decision-making
The tool will aid data-driven decision-making by ensuring that data is captured comprehensively and accurately in electronic records.

[Add the text below if the tool is interoperable with existing systems and/or will be used for multiple use cases]

Clinical System Integration: The organisation (X-on Health) has signed interface licenses with major clinical providers, including EMIS, TPP SystmOne, and thus is interoperable with existing systems.

Promotes scalability and interoperability
The tool will integrate with our existing electronic record systems and is adaptable to diverse health and care environments. The tool can therefore be applied to a wide range of use cases in our organisation.

Surgery Intellect is designed as a highly interoperable, voice-enabled AI assistant tailored for the primary care environment. Its architecture and functional capabilities support seamless integration with existing clinical infrastructures and deployment across multiple healthcare use cases.

SECTION 3 – What data do you want to use or share?

4. **Can you use anonymous data for your purposes? If not, explain why.**

☒	No, because: • The purpose of the tool is to aid individual care so identification of individuals is essential • The tool must record exactly what is being said to produce accurate outputs, which means that all data (including personal data) must be used

5. **Which types of personal data do you need to use and why?**

Data types needed will vary according to the type of conversation. The likely types have been selected below. [Review the yellow highlighted options and add any other data type you are aware will need to be included]

☒	Forename	☒	Physical description, for example height	☒ ☐	Photograph / picture of people
☒	Surname	☒	Phone number	☐ ☐ ☐	Location data e.g. • IP address • Other [please state]
☒	Address	☒	Email address	☒	Audio recordings
☒	Postcode full	☒	GP details	☐	Video recordings
☐	Postcode partial	☐	Legal representative name (personal representative)	☐	Other [please state]
☒	Date of birth	☒	NHS number	☐	None
☒	Age	☐	National insurance number		

☒	Gender	☐	Other numerical identifier [please state]			Any

personal data discussed as part of the meeting or consultation will be included in the dataset so that an accurate record is produced.

6. **Data protection laws mean that some data is considered particularly sensitive. This is called special category data. Data that relates to criminal offences is also considered particularly sensitive. Which types of sensitive data do you need to use or share?**

Data types needed will vary according to the type of meeting or consultation. The likely types have been selected below. [Review the options and select any other data type you are aware will need to be included]

Type of data		**Reason why this is needed (leave blank if not applicable)**
☒	Information relating to an individual's physical or mental health or condition, for example information from health and care records	This may be included where it is discussed as part of the meeting or consultation, as the content must be accurately recorded
☐	Biometric information in order to uniquely identify an individual, for example facial recognition	
☐	Genetic data, for example details about a DNA sample taken as part of a genetic clinical service	
☒	Information relating to an individual's sexual life or sexual orientation	This may be included where it is discussed as part of the meeting or consultation, as the content must be accurately recorded
☒	Racial or ethnic origin	This may be included where it is discussed as part of the meeting or consultation, as the content must be accurately recorded
☐	Political opinions	
☐	Religious or philosophical beliefs	
☐	Trade union membership	
☐	Information relating to criminal or suspected criminal offences	
☐	None of the above	

7. **Who are the individuals that can be identified from the data?**

   The likely options have been indicated below but there may be additional individuals who may be identified from the data depending on how the tool is used. [Select any options you are aware will need to be included]

☒	Patients or service users
☒	Carers
☒	Staff
☐	Wider workforce
☐	Visitors
☐	Members of the public
☐	Other [please state]

8. **Where will your data come from?**

   The data will be produced by the data subjects or by our staff in the meetings or consultations they participate in.

   [Include the below text if applicable]
   Data will also come from existing audio files held by our organisation that we will input into the tool.

Surgery Intellect utilises ambient voice technology to automate clinical documentation during patient consultations either face-to-face or over the phone.

9. **Will you be linking any data together?**

   [Put an ☒ next to the one that applies.

   The answer may be 'yes' if the tool will pull data together from different sources, such as from different systems]

☒	Yes [provide an explanation of why this is necessary, for example data from different systems needs to be linked together so that the tool can generate a complete and accurate summary to help inform next steps. Then go to question 9a] Surgery Intellect serves as a primary interface within the X-on Intelligent Care Navigation System, Specifically integrated into the Surgery Connect platform and phonebar desktop application. TORTUS provides the underlying artificial intelligence engine that enables: • **Ambient Voice Capture:** The technology listens to patient consultations in real-time to capture clinical dialogue. • **Automated Documentation:** TORTUS's AI processes the captured audio to generate structured clinical notes, referral letters, and clinical codes.

	• **EHR Filing:** These AI-generated outputs are then seamlessly filed into the patient's Electronic Health Record (EHR), following clinician review,via the Surgery Intellect interface.
☐	No [skip to question 10]
☐	Unsure [try to provide an explanation of what you think then go to question 9a]

a. Will it become possible, as a result of linking data, to be able to identify individuals who were not already identifiable from the original dataset?

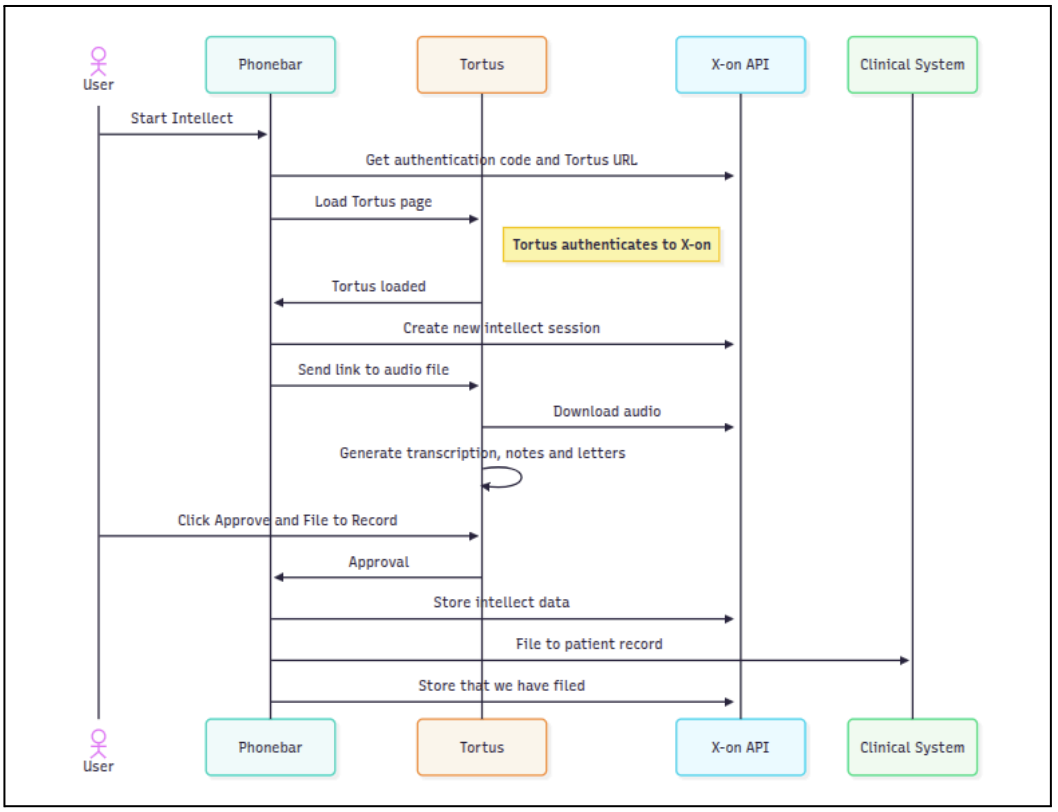
☒	No – all data input into the tool will be from existing identifiable data sources

SECTION 4 – Where will data flow?

10. Describe the flows of data.

[You can use this table - some examples have been provided. Alternatively, you can use a data flow map or a written description of the data flow. A simple example of a map could be: 'clinician - inputs audio file into tool - summary uploaded into patient's hospital record'. You will need to add details to ensure you have fully covered where the data flows from, through and to at all stages of the processing. For example, there may be a flow from the Personal Demographic Service (PDS) to pull through contact details.

The developer of the tool is likely to be able to provide you with a description or visual data flow map of how the data is input, processed by the tool and then output]



Description of Flows:

From a patient and GP perspective, the journey is designed to be seamless and nearly invisible to the patient, while hugely beneficial to the GP. Please see here for an interactive overview of the user journey:

1. Initiating the Consultation: The GP activates Surgery Intellect with one click on the Phonebar icon for the consultation.
2. During the Consultation: The consultation is being recorded with Surgery Intellect “listening” in the background
3. Consultation End and AI Note Generation: At the end, as the GP stops the recording, TORTUS quickly generates a draft note in the GP’s preferred format, with clinical codes highlighted for review.
4. Clinician Review & Edit: The GP reviews the AI-generated note, verifies medical details, and edits as needed. Additional context can be added if required, or a template style selected for instant reformatting.
5. Adding Codes and Letters: The GP reviews suggested coding (e.g. blood pressure or diagnoses), deciding which to keep. If a referral letter or advice leaflet is needed, the GP can instantly generate a draft letter populated with relevant information, saving admin time.
6. Saving to Patient Record: The GP clicks “Approve and Save”. The finalised note (and any codes) is automatically filed into the patient’s record.
7. After the Consultation: The patient leaves with no delay from note-taking, the GP may already be finished with admin as the patient departs. If needed, the GP can revisit the consultation transcript or audio. This efficiency allows for earlier completion of clinics and more time for patients.

Data flow name	**Going from**	**Going to**	**Data description**
New voice input data	Patient and clinician	AI-enabled scribing tool	The tool records the audio data (conversations) generated at the time of the meeting or consultation
Existing voice input data	Pre-recorded audio files (e.g. from digital telephony service)	AI-enabled scribing tool	The staff member uploads audio recording files into the tool for processing
Clinical review	AI-enabled scribing tool	Clinician	The staff member reviews the audio recording and output files to confirm accuracy and make amendments/decisions where needed
Tool output data	AI-enabled scribing tool (hosted on organisation’s cloud server)	Electronic patient record system	The tool processes the input data and feeds the summary output into the relevant patient record on the electronic patient record system

11. **Confirm that your organisation's information asset register (IAR), record of processing activities (ROPA) or your combined information assets and flows register (IAFR) has been updated with the flows described above.**

☒	Yes
☐	No
☐	Unsure [add as a risk in section 10 with an action to find out]

[Your organisation is required to keep a record of the types of data processing it undertakes and any information assets it holds. The template Information Asset and Flows Register (IAFR) allows you to record both of these in one register. Alternatively, you can record them separately, with types of data processing recorded in a ROPA and information assets recorded in an IAR.]

12. **Will any data be shared outside of the UK?**

☐	Yes [go to question 12a]
☒	No [skip to question 13] All storage and processing servers are within the UK.
☐	Unsure [add as a risk in section 10 with an action to find out then skip to question 13]

a. **If yes, give details, including any safeguards or measures put in place to protect the data whilst outside of the UK.**

SECTION 5 – Is the intended use of the data lawful?

[You should consider seeking advice to help you complete this section if you are not an IG professional.]

13. **Under Article 6 of the UK General Data Protection Regulation (UK GDPR) what is your lawful basis for processing personal data?**

[Note that using data that was originally collected as part of providing individual care for any further purpose, such as to support research, training the tool or any other use, will require separate consideration, and has not been included in this DPIA.]

Processing is necessary for the performance of a contract with X-on Health, processors for Surgery Intellect, powered by TORTUS. (UK-GDPR Article 6.1(b) and Article 6.1(e) for this lawful basis of processing. X-on acts as a data processor for and on behalf of the Surgery Intellect, powered by TORTUS. The GP practice remains the data controller in relation to such personal data with responsibility for communication with individuals.

☒	(e) **We need it to perform a public task** See this list for the most likely laws that apply when using and sharing information in health and care.

14. **If you have indicated in question 6 that you are using special category data, what is your lawful basis under Article 9 of the UK GDPR?**

[Note that using data that was originally collected as part of providing individual care for any further purpose, such as to support research, training the tool or any other use, will require separate consideration, and has not been included in this DPIA.]

For the processing of health data within the NHS and primary care, the lawful bases under Article 9(2) typically relied upon by the Data Controller (the GP Practice) and supported by X-on Health as the Data Processor are:

- **Article 9(2)(h):** Processing is necessary for the purposes of preventive or occupational medicine, medical diagnosis, the provision of health or social care or treatment, or the management of health or social care systems and services.
- **Article 9(2)(i):** Processing is necessary for reasons of public interest in the area of public health.

☒	(h) **We need it to comply with our legal obligations to provide or manage health or social care services** See this list for the most likely laws that apply when using and sharing information in health and care.

15. What is your legal basis for using and sharing this health and care data under the common law duty of confidentiality?

☒	**Implied consent**

a. Please provide further information or evidence.

We will ensure that people who can be identified from the data are made aware of how their data will be used. This includes informing people before engaging the tool to record a consultation or meeting. If no objections are raised, their consent to use their data in this way will be implied under the common law duty of confidentiality. If the person dissents, we will not use the tool.

SECTION 6 – How are you keeping the data secure?

16. Are you collecting information?

☒	Yes

a. How is the data being collected?

- **Ambient Voice Capture**: During patient consultations, Surgery Intellect utilises ambient voice technology (AVT) to listen to and transcribe clinical dialogue in real-time.
- **Source Integration**: Voice data is captured via the **X-on Phonebar** for both in-person (ambient) consultations and telephone consultations conducted through the Surgery Connect system.
- **Data Minimisation**: The system is engineered to capture only the information necessary to generate structured clinical notes, referral letters, and clinical codes.

17. Are you storing information?

[There may be some data that will be stored as part of the processing, for example the outputs, but not the actual recordings. The raw audio recordings may also be stored for a period of time, for example until summaries have been confirmed as accurate. Clearly indicate the data that is stored and / or data that is not]

☒	Yes
☐	No

a. How will information be stored?

[Put an ☒ next to all that apply.

[Include details on where the tool will store recordings and outputs (for example summary notes and patient letters. Clearly indicate if these are stored in different locations.]

Storage location		**Details (leave blank if not applicable)**
☐	Physical storage, for example filing cabinets, archive rooms etc	[provide details including whether the facility is operated by your organisation or a third party]
☐	Local organisation servers	[provide details]
☒	Cloud storage	All patient data is processed and stored exclusively within secure, **UK-based Tier 3 data centres**
☐	Other	[please state]

X-on Health follows the NHS data controller/processor model: the GP practice or NHS body is the Data Controller, and X-on as the Data Processor, with TORTUS as a sub-processor. Patient data is stored for the shortest possible time, always within UK/NHS-approved infrastructure. No long-term storage of patient-identifiable data occurs. For TORTUS, data is processed in real time. No audio or transcripts are stored beyond session. Temporary processing memory (browser) is cleared at logout or 24 hours. For X-on Health, call data is stored in secure 4 UK data centres (London, Manchester) for a length of time agreed per NHS Customer agreement.

18. Are you transferring information?

☒	Yes – the outputs will be transferred onto the electronic patient record system

a. How will information be transferred?

Surgery Intellect is a voice-enabled AI assistant that uses TORTUS AI ambient voice technology (AVT) to listen to patient consultations and subsequently generate medical notes, letters, and clinical codes. It works for both telephone and in-person appointments (ambient consultations). Surgery Intellect's architecture is made up of the X-on Health Surgery Connect Phonebar integrating with TORTUS AI via the X-on Health API Gateway. Existing integration with the chosen clinical system via the X-on Surgery Connect Phonebar, will enable the filing back to record of clinician reviewed, AVT generated patient notes, medical letters, and clinical coding.

The patient consultation occurs within the X-on environment, once this is finished, providing the user has clicked on the Intellect Icon, the call recording is passed on to TORTUS AI, for transcription and for the generation of the aforementioned AVT generated content.
TORTUS AI architecture:

- Speech-to-text engine: Real-time transcription performed using a self-hosted S2T model running in secure cloud containers managed by TORTUS on GCP. All processing is routed through TORTUS-controlled infrastructure.
- TORTUS AI Layer: Proprietary large language model stack used for structuring clinical notes, applying templates, extracting clinical elements (e.g. diagnoses, medications), and running hallucination/omission detection. This includes both general and fine-tuned open-source LLMs, hosted and isolated within TORTUS containers.
- Clinical Safety Layer: Independent AI routines to validate factual consistency, detect omissions, and monitor WER proxies. Integrated with clinician feedback loop and surveillance dashboard.

19. How will you ensure that information is safe and secure?

[You need to have measures in place to ensure that the data is safe and it won't be used, either on purpose or accidentally, in ways that are unlawful. The measures needed will be dependent upon, and proportionate to, the data which is being used.

Add details of the specific controls for the tool you are proposing to use]

[Put an ☒ next to all that apply.]

	Security measure	Details (leave blank if not applicable)
☒	Encryption	Audio is AES-256 encrypted and inaccessible outside the session
☒	Password protection	
☒	Role based access controls (RBAC)	[where users only have access to the data held digitally which is needed for their role (this includes setting folder permissions)]
☐	Restricted physical access	[where access to personal data is restricted to a small number of people, such as access cards or keys to a restricted area]
☒	Business continuity plans	As a constituent service of the X-on Health ecosystem, **Surgery Intellect** is governed by the same rigorous Business Continuity and Disaster Recovery (BCDR) framework that secures the Surgery Connect platform. The X-on Health strategy is certified to **ISO 22301 (Business Continuity Management)**, ensuring clinical and administrative workflows remain resilient in the face of technical or environmental disruptions.
☒	Security policies	[for example, a system level security policy. Embed these]
☐	Other	[please state]

20. How will you ensure the information will not be used for any other purposes beyond those set out in question 2?

Specify the measures below which will be used to limit the purposes the data is used for.

[Put an ☒ next to all that apply and provide details.

The appropriate type of contract or agreement will depend on the relationship that your organisation has with the tool developer, and the level of input from them. Whichever type of agreement you use, you must ensure that it is legally binding and clearly sets out the roles and responsibility of each organisation.]

Security measure		Details (leave blank if not applicable)
☒	Contract	Our organisation has entered into a legally binding contract with the developer of the tool that sets out the roles and responsibilities of both parties, including the controller and processor relationship.
☒	Data processing agreement	Our organisation has entered into a legally binding data processing agreement with the developer of the tool that sets out the roles and responsibilities of both parties, including the controller and processor relationship.
☐	Data sharing agreement	[This sets out the arrangements for sharing data between the organisations involved – it may or may not be legally binding depending on the content]
☒	Data sharing and processing agreement (DSPA)	Our organisation has entered into a legally binding agreement with the developer of the tool that sets out the roles and responsibilities of both parties, including the controller and processor relationship.
☒	Audit	The tool has audit functionality to capture who has accessed data held and generated by the tool. [Provide further details, for example the role of who will be reviewing the audit log and the frequency/trigger point for this]
☒	Staff training	We will train staff as part of our rollout to ensure they are aware how to use the tool appropriately. [Check whether the supplier will be involved in providing the training]
☒	Acceptable use policy	Our staff will need to comply with the tool's acceptable use policy. [Check whether the developer has a policy that is appropriate for you to use or if your organisation needs to develop a local policy too]
☐	Other	[please state]

SECTION 7 – How long are you keeping the data and what will happen to it after that time?

21. How long are you planning to use the data for?

We intend to start using the data on [add date] and will finish using the data on [add the contract/project/programme end date or indicate if it is ongoing.

These dates may be for when a pilot of the tool is due to go live and end, or it could be a contract start and end date.]

22. How long do you intend to keep the data?

[Add details of how long each data type will be kept for, for example, raw audio recording files, transcripts, outputs.

You must ensure that the raw input data is kept for long enough to be able to ensure that an appropriate accuracy check is done (for example, the clinician reviews the summary and clicks a button to accept it, deleting the raw audio file). A one month retention period is likely to be sufficient to cover this process but less is preferable where possible.

The retention period of the outputs is likely to align with your usual retention period for health and care records, as set out in the Records Management Code of Practice.]

23. What will happen to the data at the end of this period?

[Put an ☒ next to all that apply.]

Action		Details (leave blank if not applicable)
☒	Secure destruction (for example by shredding paper records or wiping hard drives with evidence of a certificate of destruction)	Upon the termination of the contract, X-on Health will delete confidential or sensitive data records, including call recordings. The destruction of confidential, financial, and personnel-related records shall be securely destroyed electronically or by shredding. X-on Health will provide a certificate assuring that the GDPR data retention policy has been followed.
☐	Permanent preservation by transferring the data to a Place of Deposit run by the National Archives	[Provide details of who will do this]
☐	Transfer to another organisation	[Provide details]
☒	Extension to retention period	With approved justification X-on Health will extend the retention period.
☐	It will be anonymised and kept	[Provide details of how this will be done and by who]

☒	The controller(s) will manage as it is held by them	Our organisation will manage data transferred into the electronic patient record system in line with existing practice
☒	Other – data outputs such as transcripts produced by the tool will be deleted once the outputs have been verified and accepted	X-on Health will delete confidential or sensitive records including call recordings and we shall either delete or anonymise less important documents. The destruction of confidential, financial, and personnel-related records shall be securely destroyed electronically or by shredding. X-on will provide a certificate assuring that the GDPR data retention policy has been followed.

[The Records Management Code of Practice provides detail about what happens once a retention period has been reached.]

SECTION 8 – How are people's rights and choices being met?

24. How will you comply with the following individual rights (where they apply)?

[For joint controllers, indicate anything you have agreed, such as designating one controller as a point of contact for patients and service users (data subjects).

These rights will not always apply so you should review each one to see if it applies.]

Individual right	**How you will comply (or state *not applicable* if the right does not apply)**	
The right to be informed The right to be informed about the collection and use of personal data.		We have assessed how we should inform individuals about the use of data for the tool. We will use the communication methods below, including directly informing data subjects that an AI scribe is being used at the beginning of their consultation. We consider this necessary because it is not reasonable to assume at the initial roll out of the tool that people will know the tool is being used unless we actively inform them. However, we will review this as people become more familiar with the use of this type of technology. [Put an ☒ next to all that apply.]
	☒	Privacy notice(s) for all relevant organisations [provide a link or describe where it will be displayed and embed a copy]

	☒	Information leaflets
	☒	Posters in waiting rooms and consultation rooms
	☒	Screens in waiting areas
	☐	Letters
	☒	Emails to all patients or service users to let them know existing recorded telephone conversations may be put through the tool to summarise
	☐	Texts
	☐	Social media campaign
	☐	DPIA published (best practice rather than requirement)
	☒	Banner/pop up in video consultation window
	☒	Staff will verbally inform individuals prior to processing
	☒	Other – We will directly inform data subjects that an AI scribe is being used at the beginning of their consultation. We will also include information about the use of the tool in our patient newsletters
	☐	Not applicable
The right of access The right to access details of data use and receive a copy of their personal information - this is commonly referred to as a subject access request.	Data subjects can request access by following the process on our website or speaking to a member of staff. The tool allows staff to extract and download relevant data in a format that can be easily accessed by the data subject. [add details of how this will be done]	
The right to rectification The right to have inaccurate personal data rectified or completed if it is incomplete.	Data subjects can request rectification by following the process on our website or speaking to a member of staff. There should not be a need to rectify a recording of a conversation as this should be seen as a factual capture. Where an individual disagrees with a statement within the recording, the tool has functionality to [add	

	details of how a note or adjustment can be added to any held data if agreed and necessary]. The tool provides functionality to clearly indicate where data is incorrect but still must be retained, so that inaccurate data is not used to inform any decisions in the future and the integrity of the record is preserved. The tool allows staff to amend inaccurate data outputs [add detail of how the tool provides this functionality]
The right to erasure The right to have personal data erased, if applicable.	Does not apply to this data, as it is exempted under UK GDPR Article 6(1)(e) public task. However, if the audio recording data is still held and is no longer needed (where all necessary outputs have been transferred into the electronic patient record system), the original audio recording could be subject to the right to erasure if it is no longer needed for the purpose it was collected.
The right to restrict processing The right to limit how their data is used, if applicable.	Data subjects can request restriction by following the process on our website or speaking to a member of staff. [add details of how the tool can restrict further processing of data it holds, and how data held outside of the tool, such as on the electronic patient record system, can be restricted. This includes pausing any automated processes like scheduled deletion and putting a record beyond use. We will ensure that any restriction of processing does not impact upon the individual's care, by staff manually taking notes or producing referral letters while the data is restricted.
The right to data portability The right to obtain and re-use their personal data, if applicable.	Does not apply, as the UK GDPR Article 6 legal basis is public task.
The right to object The right to object to the use and sharing of personal data, if applicable.	Data subjects can object at any time by speaking to a member of staff or by contacting our organisation. Data subjects are made aware of their right to object through the privacy notice and other published materials outlined above. Objections can be overridden where there are 'compelling legitimate grounds' to continue to process data in this way which outweigh the rights of the individual. However, this will be assessed on a case-by-case basis. This is different to an individual's decision to dissent to

	the processing, so we will take this requirement into consideration when assessing whether to uphold an objection. In practice, this means where a data subject objects to the tool being used for a specific consultation, staff will not start recording and manually take notes or produce other outputs the tool would otherwise do, if required. If the objection is raised part way through the consultation, we will stop the recording. Where a data subject completely objects to the tool's use of their data for individual care, staff will add a note to their record to say that they do not want the tool to be used. Where we have already used the tool on the basis of implied consent, the individual can no longer dissent, but the right to object will still apply and we will assess whether or not to uphold their objection.

25. Will the national data opt-out need to be applied?

☒	No – the data will be used for individual care only. Any further use of data will need to be considered separately and is not covered in this DPIA.

26. Will any decisions be made in a purely automated way without any human involvement (automated decision making)?

☒	No, you must ensure that there is always a human review of outputs, for example, confirming that the clinical SNOMED code that the tool generates is the correct one, or agreeing that a referral is appropriate. skip to question 27

27. Detail any stakeholder consultation that has taken place (if applicable).

[For example, if your processing will have a significant impact on partner organisations or the public, you may have approached them for their views and incorporated them into the design of your data use. Include any consultation with the Information Commissioner's Office (ICO) if applicable.]

SECTION 9 – Which organisations are involved?

28. List the organisation(s) that will decide why and how the data is being used and shared (controllers).

[add your organisation's name]

[The organisation(s) listed here will be making the decisions for example:

- to collect the data in the first place

- what data is being collected
- what it is being used for
- who it is being collected from

The organisation(s) will also be likely to have a direct relationship with those the data is being collected from, for example patients, service users or employees.

There may be more than one organisation listed here. They may be controllers for their own data, for example even if multiple care homes were all using the same software supplier to manage their care records, each care home would only be controller for their own residents' information. In some instances, organisations may be joint controllers. For example, this may apply where organisations are using the data for the same purpose, where you share a dataset with another organisation, or where you have designed a new collection with another organisation. An example of where there may be joint controllers in some instances is shared care records, where multiple health and care organisations are contributing data for the same purpose.]

29. **List the organisation(s) that are being instructed to use or share the data (processors).**

[This is likely to be the developer organisation, unless the tool is purely code applied to your existing system and the developer has no way of accessing or managing the data]

[The organisation(s) listed here will be under instruction from those listed in question 28, for example they are likely to be told:

- what data to collect
- who to collect data from
- how the collection is legal
- the purpose for the collection
- who to share the data with
- how long to keep the data

Where processors are not being used, state not applicable.

X-on Health Ltd

30. **List any organisations that have been subcontracted by your processor to handle data.**

In the delivery of Surgery Intellect, TORTUS AI Ltd. acts as a formal sub-processor to X-on Health Limited (the primary Data Processor).

31. **Explain the relationship between the organisations set out in questions 28, 29 and 30 and what activities they do**

[Describe here how it has been agreed that the organisations (controllers, processors and sub-processors) will work together. For example:

- Controller A (our organisation) has instructed Processor B (the developer) to provide the tool. Processor B sub-contracts the hosting of the data to sub-processor C (cloud services provider); or
- Controllers A, B and C (three hospital trust partners, as separate legal entities working jointly together to maximise resource) are controllers of their own data,

which is shared between them. They all use processor D's tool (the developer's tool)]

X-on Health is the primary Data Processor, X-on Health enters into a **Data Processing Agreement (DPA)** with the GP Practice or Healthcare Provider (the Data Controller). TORTUS is then engaged by X-on Health as a sub-processor under a mirrored agreement that ensures the same level of protection for patient data.

- **Article 28 Compliance:** The relationship is governed by UK GDPR Article 28, which mandates that the sub-processor must provide sufficient guarantees to implement appropriate technical and organisational measures.
- **Liability:** Under our standard terms, X-on Health remains fully liable to the Data Controller for the performance of the sub-processor's obligations.

TORTUS provides the underlying Artificial Intelligence (AI) and Ambient Voice Technology (AVT) engine that enables the core functionality of Surgery Intellect.

32. **What due diligence measures and checks have been carried out on any processors used?**

[Put an ☒ next to all that apply. Where multiple processors are used, indicate which option applies to which processor]

Due diligence measures		Details (leave blank if not applicable)
☒	**Data Security and Protection Toolkit (DSPT) compliance**	All certificates can be found on X-on Healths Trust Centre TORTUS (for the purposes of our third-party integration for Surgery Intellect) https://trust.tortus.ai/
☒	**Registered with the Information Commissioner's Office (ICO)**	ICO registration Z8221333 ICO Certificate
☒	**Digital Technology Assessment Criteria (DTAC) assessment**	All certificates can be found on X-on Health's Trust Centre TORTUS (for the purposes of our third-party integration for Surgery Intellect) https://trust.tortus.ai/
☒	**Stated accreditations**	All certificates can be found on X-on Health's Trust Centre
☒	**Cyber Essentials or any other cyber security certification**	Cyber Essentials and Cyber Essentials Plus Certificates can be found on X-on Health's Trust Centre
☒	**Other checks**	[please state]

SECTION 10 – What data protections are there and what mitigations will you put in place?

33. **Complete the risk assessment table. Use the risk scoring table to decide on the risk score.**

[Some examples have been added below. These should be amended and added according to your local set up.

This should include:

- Confidentiality risks - for example unauthorised or accidental disclosure of or access to personal data.
- Integrity risks - for example unauthorised or accidental alteration of personal data. Consider also how you will ensure data is accurate and up to date.
- Availability risks - for example unauthorised or accidental loss of access to, or destruction of personal data.

You must consider risks at each stage, for example when data is being transferred, when it is stored and when it is no longer needed.

Consider whether there are any responses to questions in this DPIA that are either inconclusive or insufficient.

The ICO has published an AI and data protection risk toolkit that you may wish to use]

Risk assessment table

Risk ref no.	Description	Risk score* (L x I)	Mitigations	Risk score* with mitigations applied
Accuracy risks				
01	Outputs do not represent an accurate record of the conversation which could lead to patient safety risks	16	Following the consultation and once the output has been generated, the user reviews the output to ensure they agree its accuracy, or edit the record if required Staff are able to flag or report errors, or patterns of unusual or unexpected outputs by using the thumbs up and thumbs down toggle which reports straight back to TORTUS the sub-processor.	4
02	Tool produces 'hallucinations'	16	Hallucination and Omission Rate: Critical metric tracked via audits and clinician feedback to	4

			ensure a near-zero rate of significant clinical errors. Staff are able to flag or report errors, or patterns of unusual or unexpected outputs by using the thumbs up and thumbs down toggle which reports straight back to TORTUS the sub-processor for onward investigation.	
03	Overreliance on the AI, not always checking outputs, particularly where clinical codes or clinical suggestions are generated by the tool, even if this is the intended use	16	Staff training and awareness activities to ensure staff are aware that they are accountable and responsible for their use of the AI output Monitoring of tool use X-on Health will provide in person training and online training resources which will emphasise the need for human review and sign off into the process for accepting the AI output and inputting into patient records.	4
04	Data integrity or data loss issues as the data is transferred onto local electronic record systems	16	Following the consultation and once the output has been generated, the user reviews the output to ensure they agree with its accuracy, or edit the record if required. Surgery Intellect has various failsafe windows and prompts in place before the user gets to the stage of saving to the patient record, this then makes the risk around filing inaccurate data highly unlikely.	4
05	Tool does not accurately record speech where people have strong accents or dialects, complex terminology, abbreviations or acronyms	16	Following the consultation and once the output has been generated, the user reviews the output to ensure they agree with its accuracy, or edit the record if required.	4

			Staff are able to flag or report errors, or patterns of unusual or unexpected outputs by using the thumbs up and thumbs down toggle which reports straight back to TORTUS the sub-processor.	
Availability risks				
06	Data availability if the system goes down e.g. if there is a cyber attack	16	Business continuity plan, security policies and other security measures - see question 19 for details.	4
Confidentiality risks				
07	Inappropriate access to transcripts	6	Role based access controls Secure storage of data Deletion of transcripts once purpose has been fulfilled Audit trail of all access Contractual arrangements with developer covering staff access Surgery Intellect is accessed through the X-on Health phonebar, which will hold its own access controls.	4
08	Tool records excessive information not requested by the user e.g. accidentally recording private conversations		Following the consultation and once the output has been generated, the user reviews the output to ensure they agree with its accuracy, or edit the record if required.	
Fairness risks				
09	Data subjects consider the technology to be intrusive		Transparency materials Option to not use the tool through the right to object	
10	Invisible processing, particularly if existing audio recordings are input into the tool		Transparency materials must reach all relevant data subjects [add details of what you will do, e.g. email out to all patients to	

			let them know existing recorded telephone conversations may be put through the tool to summarise]	
11	Risk that the developer uses the data for training without the Controller's knowledge or approval, including where deidentifying the data first		Contractual terms legally limiting data use by the developer	
12	Re-use of data for a non-compatible purpose such as training AI models on data originally collected for direct care		Role based access controls Staff training and awareness activities Acceptable Use Policy defines what is and is not permitted Other organisational policies and processes [provide details] Objections process available for individuals to register their objections to specific uses of their data Transparency materials Anonymisation processes may be used for secondary purposes to preserve privacy This DPIA covers use for supporting individual care. Any further uses, such as for research or planning, must be considered in a separate DPIA	
13	Users intentionally or unintentionally using the product for purposes outside of the defined and acceptable use		Role based access controls Staff training and awareness activities Acceptable use policy Staff are able to flag or report errors, or patterns of unusual or unexpected outputs	

14	Data subjects not sufficiently aware of how their data is processed, used or retained, either due to ineffective transparency, or black box processing preventing full transparency from being possible		Outputs (including decisions) to be reviewed and accepted by staff, who will be able to explain their justifications to data subjects Data subjects to be informed verbally of the use of the tool until staff are assured that the data subjects expect the processing and do not object Staff are able to flag or report errors, or patterns of unusual or unexpected outputs	
15	Unfairness or bias in training data impacting certain groups of people in particular		Large language model (LLM) performance testing [add details e.g. test cases reviewed by humans] Engagement with the developer to understand the work they have done to address this risk [add details] [add details of options for further mitigations] Staff are able to flag or report errors, or patterns of unusual or unexpected outputs	
16	Individuals hesitate or withdraw from providing full information due to a lack of confidence in the tool, particularly if they are concerned that objecting will impact their care		Transparency materials Right to object Alternative process in place to cover the tool's activities (e.g. manual note taking). Ensure these alternative processes are known to staff members and remain viable for them post-implementation of the tool.	
17	Tool does not allow all individual rights to be upheld (or makes the process difficult)		See mitigations detailed in question 24	
Other risks				

18	Running out of storage space for large volumes of data collected and generated		Engaging with the tool developer to understand storage requirements and implications when scaling up on users Deleting data once transferred to electronic record system Alternative process in place to cover the tool's activities (e.g. manual note taking) if tool becomes unavailable	
19	Legal basis may change at different stages of the processing (both for the common law duty of confidentiality and UK GDPR)		This DPIA covers use for supporting individual care. Any further uses, such as for research or planning, must be considered in a separate DPIA	

***Risk scoring table**

		Impact (I)				
		Negligible (1)	**Low (2)**	**Moderate (3)**	**Significant (4)**	**Catastrophic (5)**
Likelihood (L)	**Rare (1)**	**1**	**2**	**3**	**4**	**5**
	Unlikely (2)	**2**	**4**	**6**	**8**	**10**
	Possible (3)	**3**	**6**	**9**	**12**	**15**
	Likely (4)	**4**	**8**	**12**	**16**	**20**
	Almost certain (5)	**5**	**10**	**15**	**20**	**25**

34. Detail any actions needed to mitigate any risks, who has approved the action, who owns the action, when it is due and whether it is complete.

Risk ref no.	Action needed	Action approver	Action owner	Due date	Status e.g. outstanding/complete

SECTION 11 – Review and sign-off

[Ensure the relevant staff review or sign off the DPIA according to your governance structure. For example, this may be a more senior member of staff for higher risk processing. Add additional entries for multiple reviewers / approvers.]

Reviewer sign-off	
Reviewer name:	
Reviewer job title:	[For example, Senior Information Risk Owner, Caldicott Guardian, Information Governance Lead, Information Asset Owner, IT lead, Data Protection Officer]
Reviewer contact details:	
Date of review:	
Comments:	
Date for next review:	

Approver sign-off	
Approver name:	
Approver job title:	
Approver contact details:	
Date of approval:	
Comments: