Data Protection Impact Assessment

Tortus

Version No: 1
Status: Requiring practice and DPO service Approval

Authors: Steve Short
Approver:

Date: 04/JAN/2025

Digital Health and Care Wales
Ty Glan-yr-Afon
21 Cowbridge Road East
Cardiff
CF11 9AD

Telephone: 029020 500 500
dhcw.nhs.wales

Table of Contents

1.0 Document history

1.1 Revision history

Date	Version	Author	Revision Summary
06/01/2025	0.1		

1.2 Reviewers

This document requires reviewing by the following individuals

Date	Version	Reviewer Name	Reviewer Title
04/01/2025	0.1	Steve Short	
06/01/2025	0.1	Modupe Akinrinade	DPO Support Service Officer
04/02/2025	0.2	Rebecca Marino	DPO Support Service Lead

1.3 Approval

This document requires approval from the following individuals

Date	Version	Name	Title

Data Protection Impact Assessment Template

Section A - Project Description

To be completed by the project lead

Please complete with as much information as possible as this will assist the IG team/lead in assessing whether further action is required.

Information Asset/Project Name	TORTUS
Directorate/Department	
Organisation	Nantgawr Road Medical Centre
Is this a change to an existing process?	Yes
Assessment Completed By	Steve Short
Job Title	Salaried GP
Date	04/JAN/2025
E-mail	Steve.short@wales.nhs.uk
Information Asset Owner	
Does the project/process involve the processing of personal data? (If no, complete q1 only)	Yes

Project/Change Outline - What is it that is being planned? If you have already produced this as part of the project's Project Initiation Document, Assurance Quality Plan or Business Case etc. you may make reference to this, however a brief description of the project/process being assessed is still required.

There is currently an administrative burden on clinicians, where clinicians are taking up a lot of time to write up clinical notes after visits. Therefore, the Tortus app will be used to free up clinical administrative time for clinicians. Tortus is a desktop and web-based application which uses audio recorded during a consultation to create medical notes and letters. Clinicians can access the Tortus app on devices with in-built or connected microphones.

The key features of the Tortus app are:

- **Speech to Text:** The Tortus app transcribes the clinical consultation in bulk and produces a transcript for the clinician to review.
- **Text Summarisation:** The Tortus app restructures the data from the transcript into a template medical summary, following a specific format e.g. a Subjective, Objective, Assessment, and Plan (SOAP) note. The output is a summary medical history note for the patient, to be checked by the clinician.
- **Letter Generation:** The Tortus app uses the data from the summarisation and produces a letter from a set template, to be checked by the clinician.

The Tortus app is currently only intended for use by clinicians and health professionals during outpatient hospital clinical consultations and primary care settings. Clinicians are expected to check the accuracy and completeness of:

- Transcriptions

- Summarisations
- Letters

In addition, clinicians are expected to ensure they transfer (i.e. copy and paste) any outputs of Tortus to the patient's Electronic Patient Record / EMIS Web

All data processed within the Tortus app, including any sharing of data, is determined by the data controller. The data processed within the Tortus app is an audio recording initiated by the clinician, with all audio then captured during the clinical consultation. Recordings can be initiated, paused and stopped by the clinician and the Tortus app provides visual feedback to users to indicate when the recording is active.

Information will be primarily sourced from the conversation between clinicians and patients during consultations, which may be informed by information sourced from available electronic records, paper records or other clinical and operational systems accessed by the clinician during a consultation.

Purpose / Objectives - Why is it being undertaken? This could be the objective of the process or the purpose of the system being implemented as part of the project.

The primary purpose of this implementation is to reduce the administrative burden currently placed on clinicians in documenting patient consultations. By implementing the TORTUS application, clinicians will have their spoken consultations transcribed, summarised, and formatted into clinical notes and letters. This will streamline the documentation process, allow clinicians to focus on patient care rather than manual record-keeping, and ensure consistent, standardised formats for clinical documentation. Ultimately, the objective is to increase efficiency in clinical practice, improve the quality and consistency of patient records, and enhance overall clinical workflows without compromising accuracy or patient safety.

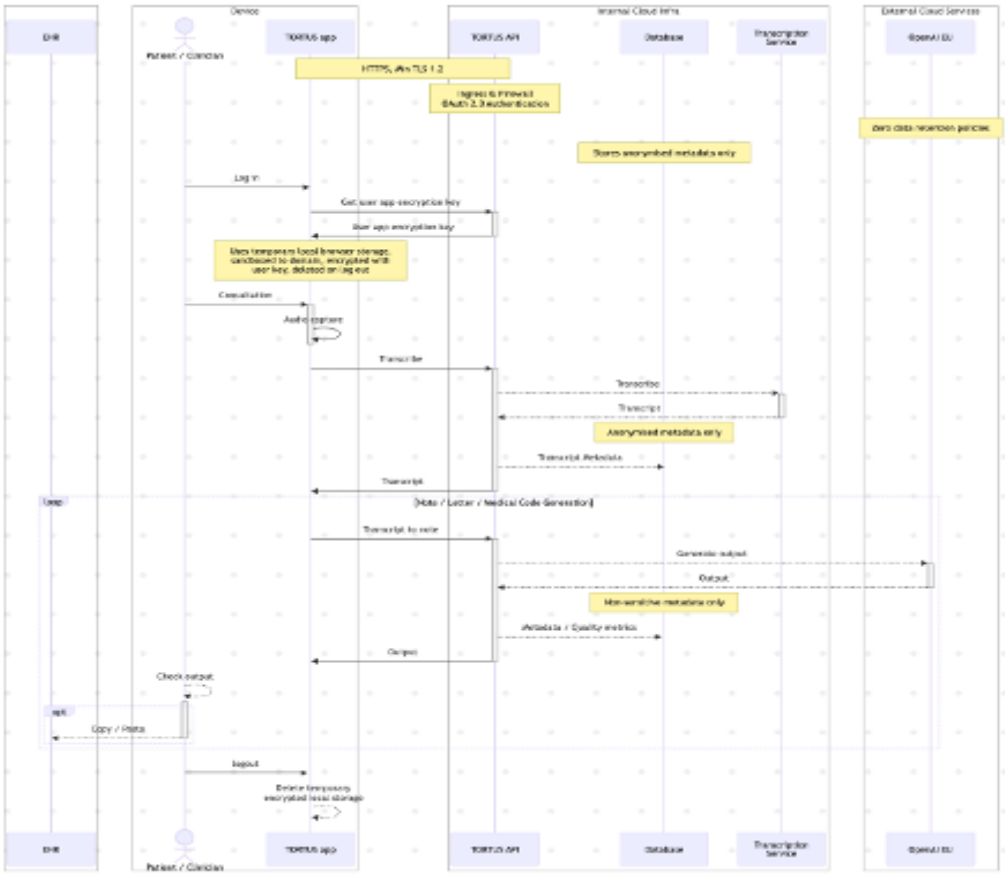
What is the purpose of collecting the information within the system? For example patient treatment, patient administration, research, audit, reporting, staff administration etc.

The purpose of using Tortus to collect and process patient data in this way is to support clinicians within clinics by transcribing audio during consultations with patients, using Artificial Intelligence (AI) to produce a summary of the consultation for inclusion within the patient record and generating letters based on the summaries produced. The Tortus app performs the task of documentation and composition of notation and letters clinicians would otherwise type in their role in delivering care. The purposes of processing are therefore likely to be the same as those already undertaken by healthcare providers - direct care.

The Tortus app is an ambient intelligent tool, hosted securely on specialist-compliant server systems, and uses enterprise-grade secure AI servers. Each session of the Tortus app begins with a blank application window. If a user accesses the system inappropriately i.e. does not log in with verified details, they are presented with a blank system chat and have no access to data. No patient data is stored by Tortus.

The specific purposes of processing are to be determined by the data controllers, however, as stated above it is intended to be used to support direct patient care.

Provide a description of the information flows (preferably including a diagram). Even if detailed information is not available some indication must be provided; this may already be available through requirements gathering. Broadly speaking the aim is to establish: who the information will be made available to, what type of information, why the information is required, how it will be shared and how often.



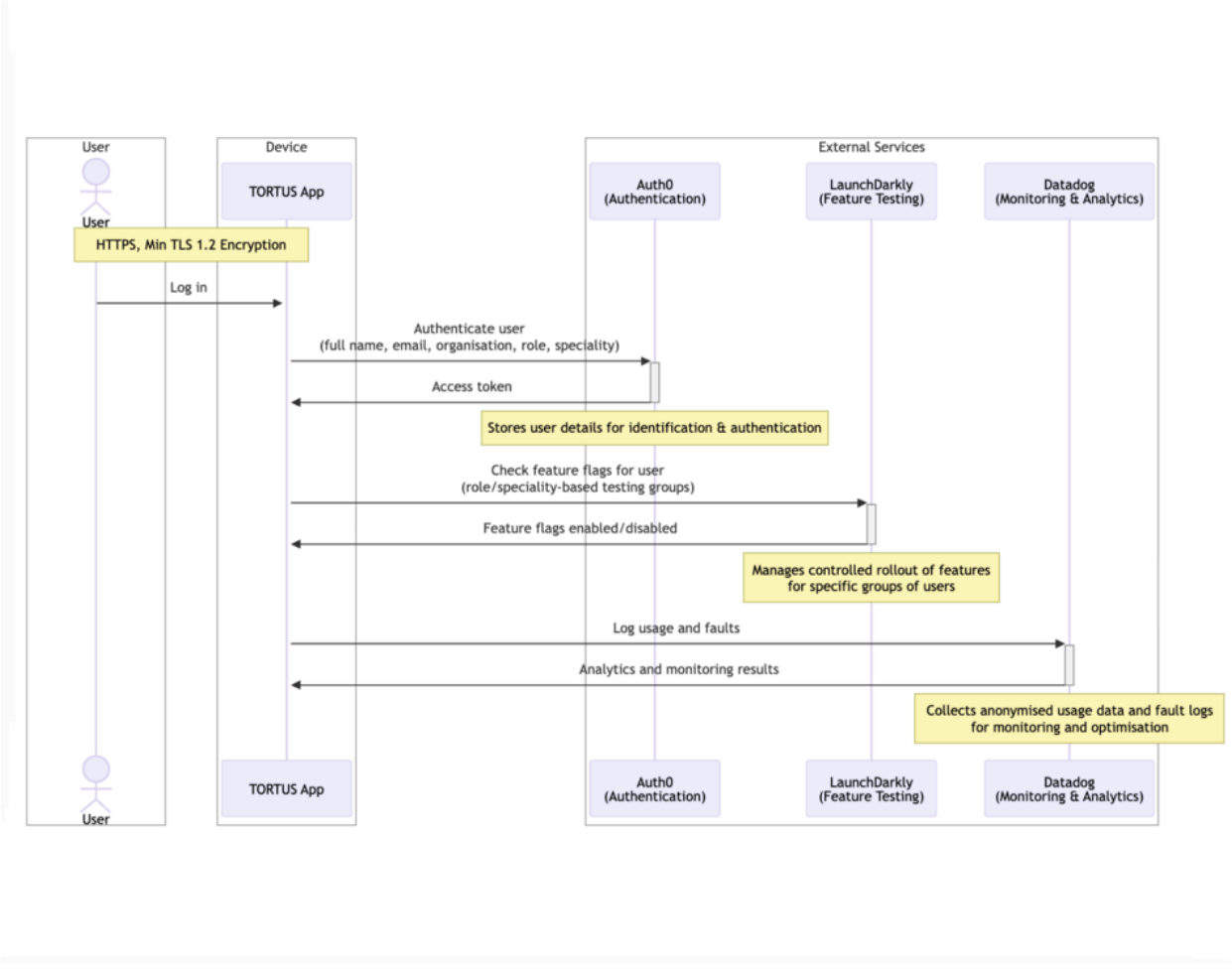
- The transcript is sent over a secure connection to the Tortus app API.
- It is then sent via the Tortus app API to OpenAi, to create a summarisation (e.g. a medical note in SOAP format) or letter.
- The summarisation is re-identified by re-inserting any items of PHI which were originally removed from the transcript.
- The clinician verifies the content of the summarisation/letter and edits as required.
- The summarisation/letter can then be copied and pasted as a medical note into other relevant systems utilised by the clinician as part of existing workflows (e.g. EMIS Web), email system, etc.
- Audio recordings are automatically deleted from the user's computer when the user logs out of the Tortus app. The audio recordings, transcriptions, summarisation and letters are not stored in any cloud services or databases by the Tortus app. The text content generated by the Tortus app is intended to be manually copied from the Tortus app by the user after verification, to any relevant systems they may use in their practice.

In addition to the data processed for clinical purposes, the Tortus app processes user data to facilitate access and feature testing. This includes storing the full name, email address, organisation, role and speciality of users via Auth0 for identification and authentication purposes. Additionally, LaunchDarkly is used to release features to specific groups of users for testing purposes, ensuring a controlled rollout of new functionality. Datadog is used for analytics and monitoring of usage and faults.

Please see details below:

1. **Authentication with Auth0:**
    - The user logs in through the TORTUS app.
    - User details such as full name, email, organisation, role, and speciality are sent to Auth0.
    - Auth0 processes the details for identification and authentication and returns an access token to the app.
2. **Feature Testing with LaunchDarkly:**
    - Once authenticated, the TORTUS app communicates with LaunchDarkly to check which features are enabled for the user.
    - LaunchDarkly determines feature flags based on user attributes (e.g., role, speciality) and returns the feature settings.
3. **Analytics and Monitoring with Datadog:**
    - The app sends anonymised usage data and fault logs to Datadog for monitoring and analytics.
    - Datadog processes the data to provide insights on usage patterns and system issues.

These data points are securely stored and managed in compliance with the relevant data protection legislation and regulations.



Provide details of how the development will have the potential to impact on the confidence patients/service users have in the NHS maintaining the confidentiality of their personal data. For example, it could be that specific information is being held that hasn't previously, the level of information held about an individual is increasing or information is being shared with another organisation through a shared system or database where it wasn't previously.
Implementing the Tortus app may introduce new privacy concerns for patients by increasing the volume and detail of personal information captured, including special category data as defined under Article 9 of the GDPR. Such data, which may include highly sensitive health details, requires additional protections due to heightened risks to individuals' rights and freedoms if disclosed without authorisation. Patients may feel uneasy about how their audio data is recorded, processed, accessed, or potentially misused, emphasising the importance of robust technical and organisational measures, legal compliance, and strong governance to maintain trust and uphold confidentiality.
Provide details of any previous Privacy Impact Assessment or other form of personal data compliance assessment done on this initiative. If this is a change to an existing system, a PIA may have been undertaken during the project implementation
N/A
Stakeholders - who is involved in this project/change? Please list stakeholders, including internal, external, organisations (public/private/third) and groups that may be affected by this system/change in the table below and detail any stakeholder activity taken.

Organisation	Engagement / Stakeholder Activity
Nantgarw Road Medical Centre	Data Controller
Tortus App	Data Processor
Google Cloud Platform	Third Party
OPEN AI	Third party
Datadog	Third party
Launch Darkly	Third party

Stakeholders - Has the patient (or group that the system is designed to hold data on e.g. employee) been consulted on the project?
☐Yes ☐No Forum the patient or other was consulted on ……

Data Types

In order to understand the potential risks to individual's privacy, it is important to know the types of data that will be held and/or shared. Even if exact detail is not known and initial indication will assist in the privacy impact assessment.

Personal	Tick (All that Apply)	Special Category	Tick (All that Apply)
Name	x☒	Racial / ethnic origin	x☒
Address (home or business)	x☒	Political opinions	☐
Postcode	x☒	Religious beliefs	x☒
NHS No.	x☒	Trade union membership	☐
Email address	x☒	Physical or mental health	x☒
Date of birth	x☒	Sexual life	x☒
Reference number (please detail)	☐	Biometrics; DNA profile, fingerprints	☐
Driving Licence [shows date of birth and first part of surname]	☐		
Bank, financial or credit card details	☐		
Mother's maiden name	☐		
National Insurance number	☐		
Tax, benefit or pension Records	☐		
Criminal offences	x☒		
Employment, school, Social Services, housing records	x☒		
Data of a "higher" sensitivity (tick all that apply)			
Abortion, Pregnancy, Embryology and Fertilisation	x☒	Sample types to include urethral swab and semen sample	x☒
Mental Health	x☒	Cervical Cytology screening	x☒
HIV/AIDs and sexually transmitted BBV's	x☒	Adoption	x☒
Genetic (also special category data)	x☒	Child Protection	x☒
Sexually transmitted diseases	x☐	Safeguarding Adults	x☒
Comments and Additional data types (if relevant):			
The types of personal data selected above may be divulged through the use of the Tortus app during clinical consultations. This is necessary for the delivery of direct care by clinicians.			

Section B - Privacy Impact Assessment Table

The project lead should complete the ‘Response’ box for each question.

The IG lead will then complete the ‘Risk Type’ and ‘Outcome’ box

Guidance Notes:

Response - Please answer the questions as fully as possible. If you are unsure of how to answer the question, please contact the IG Team. If there is supporting information that relates to any of the questions, which you feel would be informative, indicate within the comments section and send this along with the completed assessment.

Additional guidance notes have been provided for some questions; once completed the guidance notes can be removed.

The assessment table is designed to be a ‘working document’ that can be added to at intervals throughout the process, for example bullet points or rough notes can be used. These notes can be used to highlight things that need to be followed up; noted requirements can be marked up ready for the requirement schedule, etc.

Risk Type – The IG lead will use the guidance notes in Appendix 1 to identify the type of risk, this will help the organisation to judge the level of risk and either accept it or put in place appropriate measures to mitigate it.

Outcome – The IG lead will use the information provided to decide if any potential IG risks are identified. If, following discussion with the project manager/lead it is agreed there is an IG risk that requires further action the risk will be transferred onto the IG requirements schedule. The risk will be scored and progress against the identified mitigations captured using a red/amber/green status.

Section B – Privacy Impact Assessment Table [Tortus

1. Is there any data processed and/or stored in the cloud?		
Guidance Note: *Please complete*  Cloud%20Computing%20Assessment%20v		
Response (completed by project lead)	**Risk type (completed by IG Lead)**	**Outcome (completed by IG Lead)**
Yes - Tortus processes data in the Cloud as described below: **Transcription** • The Tortus app listens to the patient-doctor consultation and records audio to a local file on the clinician's computer. • The recording is sent over HTTPS to the Tortus app API hosted on Google Cloud Platform (GCP), secured by an API gateway with authentication, to a private dedicated Speech to Text model, (hosted on GCP cloud). • The transcription is returned to the Tortus app. **Summarisation/Letter writing** • The transcript is sent over a secure connection to the Tortus app API. • Transcript is sent via the Tortus app API to OpenAi, to create a summarisation (e.g. a medical note in SOAP format) or letter. • The summarisation is returned to Tortus API. • The clinician verifies the content of the summarisation/letter and edits as required. • The summarisation/letter can then be copied and pasted as a medical note into other relevant systems utilised by the clinician as part of existing workflows (e.g. EMIS Web), email system, etc. • Audio recordings are automatically deleted from the user's computer when the user logs out of the Tortus app. The audio recordings, transcriptions, summarisation and letters are not stored in any cloud services or databases by the Tortus app. The text	☐ Individual ☒Organisational ☒ Compliance	

content generated by the Tortus app is intended to be manually copied from the Tortus app by the user after verification, to any relevant systems they may use in their practice. The only data stored in the cloud as part of the transcription process relates to anonymised user interactions (e.g. the number of transcriptions/summarisations/letters, etc.). Audio recordings (sensitive data) is processed via the Tortus app is stored on the user device temporarily in memory or session state on the client (or file in the user's local directory, in the case of audio recordings). All data stored locally by the Tortus app on the end user's computer is deleted upon logout from the Tortus app.		

2. Where will the information be held and who will have responsibility for it?

Guidance Note: *Detail which team or organisation has responsibility for the system that holds the data. Detail which team or organisation has responsibility for the storage of the data. Detail how the servers are configured and Resilient. Detail which team or organisation is responsible for the security of the server the data is located on. Where is the server physically located?*

Response	Risk type	Outcome
It is expected that data controllers will require clinicians who utilise the Tortus app to ensure the summarisations and letters generated via the system are copied and pasted into the primary record for the relevant patient (e.g. held with the existing electronic health record). This will ensure the data can be retained by the data controller in accordance with the **Records Management Code of Practice for Health and Social Care** and any local record-keeping/retention policies or procedures.	☒ Individual ☒ Organisational ☐ Compliance	Risk Identified - Risk of misfiling a patient's consultation's summarisation into another patient's file.

3. What types of information will be held and/or shared?

Guidance Note*: For example, diagnostic, care plan, clinic correspondence, screening programmes, immunisation records, child health, reference data, pharmacy records etc. Will the records be electronic or paper?*

Response	Risk type	Outcome
All data processed within the Tortus app is sourced directly from conversations between clinicians and patients during consultations. The content of those conversations will be determined by the clinician and patient and the circumstances in which the Tortus app is used will be determined by	☐ Individual ☒ Organisational ☐ Compliance	Risk Identified - Risk of loss of control where data is passed outside of NHS

the customer as the data controller. This will vary from customer to customer depending on their requirements. This is however expected to include the following personal data items: **Patients, families and carers:** Personal data • Names • Addresses • Dates of birth • Telephone Numbers • Email addresses • NHS Numbers Special categories of personal data • Health data • Data which are subject to a common law duty of confidentiality • Health data **Healthcare professionals involved in the patient's care:** Personal data • Names • Job titles Conversations which are captured, transcribed and summarised will likely include personal data and special categories of personal data which are subject to a common law duty of confidentiality meaning the processing has the potential to be high risk. No paper records will be utilised through the use of the Tortus app and all processing will be electronic.		

4. Will any of the following activities be involved (tick those that apply):	
☒ Recording of demographic data ☒ Sharing of patient information ☒ Diagnostic activity results	☒ Reporting of patient activity ☒ Transfer of patient identifiable data: to other systems, to patients, to GPs or other third parties ☐ Other

5. What legal basis for processing will you be relying on? Please tick one for personal data and one for special category data (if processing). Please speak to your information governance team if unsure.

Personal Data		Special Category Data (includes health data)	
Task carried out in the public interest or in the exercise of official authority – Art 6(1)(e)	☒	Provision of preventative or occupational medicine, health or social care or treatment, or the management of health or social care systems – Art 9(2)(h)	☒
Protection of vital interests – Art 6(1)(d)	☐	Vital interests of the data subject or a third party where they are incapable of giving consent – Art 9(2)(c)	☐
Necessary for compliance with a legal obligation – Art 6(1)(c)	☐	Necessary for reasons of substantial public interest - Art 9(2)(g)	☐
		Public health - Art 9(2)(i)	☐
Consent – Art 6(1)(a)	☐	Explicit Consent – Art 9(2)(a)	☐
Other (please detail)	☐	Research – Art 9(2)(j)	☐
		Other (please detail)	☐

Outcome

Common Law Duty of Confidentiality satisfied (implied consent) for direct care

Art 9(2)(h) requires a schedule from Data Protection Act 2018:
Schedule 1, Part 1,3:
Health or social care purposes
2(1)This condition is met if the processing is necessary for health or social care purposes.
(2)In this paragraph "health or social care purposes" means the purposes of—
(a)preventive or occupational medicine,
(b)the assessment of the working capacity of an employee,
(c)medical diagnosis,
(d)the provision of health care or treatment,
(e)the provision of social care, or
(f)the management of health care systems or services or social care systems or services.
(3)See also the conditions and safeguards in Article 9(3) of the GDPR (obligations of secrecy) and section 11(1).

6. Will the planned use of personal data be covered by information already provided to individuals or is a new or revised communication planned or required?

***Guidance Note**: 'Fair Processing' i.e. informing individuals of what is happening to their information is a requirement under Data Protection Legislation. What are the existing communications? What are the planned communications?*

Response	Risk type	Outcome

The primary purpose of the Tortus app is to support the direct care of individual patients and is intended to support existing operational processes associated with note-taking, summarisation and letter production for clinical consultations. It is therefore expected that appropriate content will already exist within existing privacy notices, although consideration will be made for enhancements to these by making explicit reference to the use of technology and AI tools to support patient care.	☐ Individual ☒ Organisational ☐ Compliance	Risk Identified - There is a risk that individuals will not be appropriately informed about the processing and use of AI. Individuals need to be kept informed of how the practice is processing their personal data. Practice will need to include use of technology and AI tools for processing in their privacy notice

7. Will the development enable the sharing of records with other organisations? How will records be shared?

***Guidance Note**: Will information be transferred to a central hub with a collated record made available to participating organisations? Will participating organisations be provided with a view of records created in another organisation?*

Response	Risk type	Outcome
No, all data processed within the Tortus app, including any sharing of data, is determined by the data controller.	☐ Individual ☐ Organisational ☐ Compliance	

8. Will the development result in the handling of a significant amount of new data about each person, or significant change in existing data holdings? Please detail the new data handled.

***Guidance Note**: i.e. Is more information held about the same population of service users?*

Response	Risk type	Outcome
No, all data processed within the Tortus app is sourced directly from conversations between clinicians and patients during consultations. No additional information will be held about the same population of service users.	☐ Individual ☐ Organisational ☐ Compliance	

9. Will the development result in the handling of new data about a significant number of people, or a significant change in the population coverage? Please detail the new population

***Guidance Note**: Is the change collecting a similar data set that is currently collected but covering a different or larger population of service users?*

Response	Risk type	Outcome

No	☐ Individual ☐ Organisational ☐ Compliance	

10. Does the project involve new linkage of personal data with data in other collections, or significant change in data linkages? Please list the linking systems

***Guidance Note**: Is the development dependent on, or does it link to other systems such as Welsh Demographic Service, Master Patient Index, Welsh Results Reports Service, Welsh Care Records Service? Will the NHS Number be used as the common identifier? If not how will records be matched/linked. What measures will be in place to correctly match/link records?*

Response	Risk type	Outcome
No	☐ Individual ☐ Organisational ☐ Compliance	

11. What security controls will be in place to prevent unauthorised or unlawful processing of information?

***Guidance Note:** Describe any such measures (e.g. system controls such as role-based access, break glass, audit notifications, etc.) and outline any possible implications?*

Response	Risk type	Outcome
Encryption: All patient data is fully encrypted in transit (TLS 1.2) and at rest (AES 256 Encryption). All data is held on hardware-encrypted media. **Password protection:** • Passwords must be at least 12 characters long and must contain at least one uppercase, lowercase, number and symbol. • The system hides passwords by default. • All user accounts are subject to email verification before they are activated. • The system gives professional users limited attempts (5) to enter their password correctly before locking their account for 15 minutes. • If a professional user enters their account details incorrectly, the system conceals whether the username or password has been entered incorrectly.	☐ Individual ☐ Organisational ☐ Compliance	

• Passwords are stored salted and hashed, using algorithms and strengths recommended in NIST Cryptography Standards. • Professional user passwords are not set to expire at a certain point and changes are only required when there has been actual or potential compromise. • Professional users are able to change or reset their own passwords directly. **Role based access controls (RBAC):** Users only have access to the data held digitally which is needed for their role (this includes setting folder permissions) and users will only have access to Tortus if they have been authorised by the data controller. **Security Policies:** • Data Security and Protection Policy • Information Security and Risk Management Procedures • Information Management Procedures • Data Protection Incident Reporting and Management Procedure • Cyber Security Procedure These policies are available upon request. **Audit Notifications:** TORTUS enables and supports investigations for any reason (e.g. inappropriate access or cyber security incident). It allows for the identification of authorised users and the date and time of last access. **Google Cloud, AWS and Microsoft Azure are all ISO27001 certified meaning the underlying infrastructure on which the Tortus app system is built is all ISO27001 certified.** Break – glass functionality is already built within clinical system to alert senior members of the team if highly sensitive information has been accessed. This is fully audited should a patient's record be accessed as part of the consultation and as a result then captured as part of the transcription		
12. How is access to the system managed?		

***Guidance Note**: Who authorises accounts, manages role based access and disables accounts? Please detail who is responsible for the business processes*		
Response	**Risk type**	**Outcome**
All access to and use of TORTUS is determined by the customer (the data controller). TORTUS can be accessed using a single-factor username (email address) and password. Data Controllers must nominate one or more Admin users who will then be responsible for managing all access to TORTUS through the creation and deletion of accounts. All Admin accounts must be configured by TORTUS on behalf of the data controller.	☐ Individual ☐ Organisational ☐ Compliance	Risk Identfied - There is a risk that staff access to the system will not remain up to date. The practice will need to ensure a process is in place for: ● Creation of new accounts for new starters ● Change of access levels ● Revoking of accounts for leavers
13. What additional controls will be in place to deal with information of a higher sensitivity?		
***Guidance Note:** This includes the nationally agreed 'Highly Sensitive Conditions'; abortion, HIV/AIDS, STDs, gender reassignment, human embryology and fertilisation. Consideration must also be given to name changes through adoption, public protection or gender change and health records relating to genetics, mental health, and occupational health.*		
Response	**Risk type**	**Outcome**
The security measures detailed above will be in place to ensure that information of a higher sensitivity will be processed and stored securely. As mentioned above, Break – glass functionality is already built within clinical system to alert senior members of the team if highly sensitive information has been accessed. This is fully audited should a patient's record be accessed as part of the consultation and as a result then captured as part of the transcription	☐ Individual ☐ Organisational ☐ Compliance	
14. What are the retention periods for the personal information and how will this be implemented?		
***Guidance Note**: Retention periods for health records are set out in the Records Management Code of Practice http://systems.digital.nhs.uk/infogov/iga/rmcop16718.pdf . Within the record keeping system, there must be a method of deciding 'what is a record?' and therefore 'what needs to be kept?' This is described as 'declaring a record'. A declared record is then managed in a way that will hold it in an accessible format until it is appraised for further value or it is destroyed, according to retention policy that has been adopted.*		

Response	Risk type	Outcome
No personal data is retained within the Tortus app beyond the current session with all data being deleted upon logout from the Tortus app application. It is expected that data controllers will require clinical users of the Tortus app to copy all summarisations and letters generated via the system into the primary Electronic Health Record (EHR) for the relevant patient. This will ensure the data can be retained by the data controller in accordance with the Records Management Code of Practice for Health and Social Care and any local record-keeping/retention policies or procedures.	☒ Individual ☒ Organisational ☐ Compliance	Risk Identified - There is a risk of loss of data by deletion if an admin logs out without copying the summarisations generated via the Tortus App

15. How will you action requests from individuals for access to their personal information (in accordance with their rights)?

***Guidance Note**: Under relevant Data Protection Legislation, individuals have a right to ask for a copy of information held about them. If this is a shared record it must be established who will be responsible for dealing with the request.*

Response	Risk type	Outcome
The Tortus app temporarily stores personal data locally on the user's device but does not retain audio recordings, summarisations or other outputs beyond the current session with all data being deleted upon logout from the Tortus app. It is therefore expected that data controllers will require clinical users of Tortus app to copy all summarisations and letters generated via Tortus app into the primary Electronic Health Record (EHR) for the relevant patient. This will ensure the data can be retained by the data controller alongside other patient records and in accordance with the Records Management Code of Practice for Health and Social Care and any local record keeping/retention policies or procedures. Most importantly, this approach will also ensure that existing processes employed by the data controller for upholding the majority of data subject rights (access, rectification, erasure, restriction, portability and objections), will continue to apply to personal data processed via the Tortus app. Tortus AI Ltd can provide the following assurances to demonstrate that it has sufficient organisational and technical controls in place to adequately manage the risks to the rights and freedoms of data subjects to the data controller:	☒ Individual ☒ Organisational ☐ Compliance	Risk Identified – Should the practice temporarily store personal data that has been copied and pasted from the Appon the user's device that is not the patient's medical records, then there is a risk of unauthorised access within that 'short' period of time

• The Tortus app is compliant with the NHS Digital Technology Assessment Criteria (DTAC). • Tortus AI Ltd holds a current ICO registration: ZB512995. • Tortus AI Ltd is not subject to any ICO fines or undertakings. • Tortus AI Ltd holds an NHS Data Protection and Security Toolkit (DSPT) for the current year to 'Standards Exceeded' (ODS Code: O2G5U). • The Tortus app has undergone penetration testing with all identified vulnerabilities addressed including Open Web Application Security Project (OWASP) Top 10 vulnerabilities. • Tortus AI Ltd holds the Cyber Essentials Plus Certification.		

16a. What reporting arrangements will be in place for this service system, how will reports be generated, by whom and how will access to personal data for reporting purposes be managed?

Guidance Note: *For example, will any third parties have direct access to personal data via servers and how will the project/programme/service ensure that appropriate access controls (such as two factor authentication) are in place? What governance arrangements are in place to oversee reporting requirements and ensure that appropriate security controls are in place?*

Response	Risk type	Outcome
No third parties will have direct access to personal data via servers.	☐ Individual ☐ Organisational ☐ Compliance	

16b. What secondary data flows* are in place and have they been mapped with DHCW Information Services Directorate**?

Guidance Note: **Is the intention to use any of the following categories of data for secondary purposes – i.e. anything other than direct care or local reporting by stakeholders (i.e. reporting on their patients/clients to manage their own services)? For example, is there any intention to combine data sets from this service/system with data sets from other sources? Who agreed this? What governance mechanisms are in place to review these flows of data?*

i) personal data,

ii) pseudonymised data or

iii) aggregated / anonymised data
***Has the Project Lead established contact with DHCW Information Services to inform them of a new regular contacted Information Services to inform them of a new regular flow. Contact point: Planning and Coordination Officer, Information Services and Business Development Support Manager, Information Services*

Response	Risk type	Outcome
No.	☐ Individual ☐ Organisational ☐ Compliance	

17. How are users to be trained in their information governance responsibilities? Have any training needs been identified in addition to the mandatory NHS Wales Information Governance training? Please detail training in full.

Response	Risk type	Outcome
No additional specific IG training related to TORTUS.	☐ Individual ☒ Organisational ☒ Compliance	Admins/users of the Tortus system should be trained on how the system works

18. Is the information you are using likely to be of good enough quality for the purpose it is used for?

***Guidance Note**: Consider the flow process, and how often, the information is checked for accuracy and are there procedures to support this? Will the NHS number be used as the primary patient identifier? Is there is a likelihood that data cleansing and records reconciliation will take place? Is there is a facility to deal with data inaccuracies? Is there a facility to record the source of the information?*

Response	Risk type	Outcome
Yes, to ensure the quality of transcriptions and summarisations Tortus app contains an extensive rules engine and, through complex data handling and an inbuilt data quality module, the Tortus app validates data, highlighting any data inconsistencies. To ensure the accuracy of all transcriptions, summarisations and letters generated via the Tortus app, clinicians should be required to review all outputs generated by the Tortus app.	☒ Individual ☒ Organisational ☐ Compliance	Risk of users/admins not thoroughly reviewing the transcriptions made by the Tortus App. Practice will need to ensure that users of the App adhere to the instruction to review transcriptions and summaries before transferring to patient's records. Hence, the need for training on how the App works.

19. Will the project involve any data migration or transfer of records from other systems/new feeds? If so will the system origin and whether they were digitally born be captured in the metadata as part of the transfer process?		
Guidance Note: *If the project involves any data migration, new feeds? If so, what are the identifiers used? Will the data be maintained in an accessible format? Will the relevant metadata be captured such as whether the information is scanned in, the author, scanner, transcriber, system origin etc.*		
Response	**Risk type**	**Outcome**
No data migration or transfers of records from other systems/new feeds will take place. All data processed within the Tortus app is collected from the data subject during clinical consultations. All data processed via the Tortus app is transferred to the primary patient record/EPR/EHR/clinical system by the clinician (copy and paste) to ensure that the data controller's existing data subject rights request procedures will apply directly to the data processed via the system.	☐ Individual ☐ Organisational ☐ Compliance	
20a. Does the system maintain a comprehensive audit trail of user activity and how will the audit log be accessed and analysed?		
Guidance Note: *Will the system need to connect to National Intelligent Integrated Audit Solution? Who will be responsible for auditing? Will additional or new organisational processes be required to meet the requirement to audit all user access.*		
Response	**Risk type**	**Outcome**
Yes, the Tortus app enables and supports investigations for any reason (e.g. inappropriate access or cyber security incident). It allows for the identification of authorised users and the date and time of last access.	☐ Individual ☐ Organisational ☐ Compliance	
20b. If this is a system that has been identified as requiring full NIIAS integration, please detail the name of the new audit log event types and the date they will come available.		
Guidance Note: *Project Leads will need to discuss what audit events are generated by any given system with those responsible for its new or ongoing development*		
Response	**Risk type**	**Outcome**
N/A Name of new audit log events:	☐ Individual ☐ Organisational ☐ Compliance	

Approximate anticipated date when audit events will become available:		

21. Will the information be transferred (electronically, physically or by other portable means) to an organisation outside of NHS Wales? Please list the organisations.

Guidance Note: *where it will go and what security arrangements will apply (e.g. encryption)? Will removable media be used? Using which method will the information be transported (e.g. telephone, post, secure file sharing portal, email)?*

Response	Risk type	Outcome
Data will not be shared with any other organisations outside of NHS Wales apart from its sub-processors as outlined in this DPIA. When data is processed through the Tortus app, Tortus AI Ltd applies a range of security measures within the Tortus app to ensure the security of data in transit: • Data is securely transmitted between endpoints, Tortus app and other services (e.g. via HTTPS, WSS, SSL/TLS, etc.) • Tortus AI Ltd undertakes regular (minimum yearly) penetration testing and ensures that 'data in transit' is within scope.	☐ Individual ☐ Organisational ☐ Compliance	

22. Are there business continuity and disaster recovery plans in place to recover information which may be damaged or lost through human error, computer virus, network failure, theft, fire, flood or other disaster?

Guidance Note: *Has this been agreed as part of the Service Management arrangements?*

Response	Risk type	Outcome
Yes, Tortus AI Ltd has a Business Continuity Plan in place in line with the NHS Data Security and Protection Toolkit (DSPT) requirements. Tortus AI Ltd also has component-level disaster recovery in place with Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO), these are routinely tested. Tortus' BCP defines its critical business risks and our risk assessment process alongside organisational accountabilities.	☐ Individual ☐ Organisational ☐ Compliance	

23. Are there any elements of the system or service that are provided by a third party?

Guidance Note: *Is there a contractor (and any sub-contractors?) If so please document who the contracting authority is, who the contractors are and the confidentiality provisions within the contract, please note whether they have been subject to the information governance procurement processes, and whether they are registered with the information commissioner*

Response	Risk type	Outcome
Yes, Tortus AI Ltd utilises the following sub-processors in the delivery of	☐ Individual	

the Tortus app:

Entity	Category	Due Diligence/Assurance
Google Cloud Platform (including Vertex AI)	Software as a Service (SaaS)	ICO Registration: Z6647359 ISO27001 Certified Cyber Essentials Plus Certified NHS DSPT: 8JE14 Privacy Notice: https://policies.google.com/privacy Servers based in UK
OpenAI	Software as a Service (SaaS)	ICO Registration: ZB625491 SOC2 and SOC3 certified OpenAI has a Trust Center with comprehensive compliance documentation highlighting our robust security practices. Please request access at https://trust.openai.com/ Privacy Notice: https://openai.com/policies/row-privacy-policy/ Servers based in Ireland (EU)

☐ Organisational
☐ Compliance

All data processors engaged by Tortus AI Ltd operate under data processing agreements which meet the requirements of the Data Protection Act 2018 (and UK GDPR).		

24. Does the development involve the use of new or inherently privacy invasive technologies?

Guidance Note: *For example: smart cards, radio frequency identification (RFID) tags, biometrics, locator technologies and intelligent transportation systems, visual surveillance, digital image and video recording, profiling, data mining, and logging of electronic traffic.*

Response	Risk type	Outcome
No, the use of technology to support transcription and summarisation of audio is not novel and transcription software has been used within healthcare for many years. The Tortus app uses established technical tools, technology providers and mechanisms and has adopted best practices with respect to information security.	☐ Individual ☐ Organisational ☐ Compliance	

25. Is automated decision making involved?

Guidance Note: *Is there any profiling involved? Can there be any human intervention if required?*

Response	Risk type	Outcome
No	☐ Individual ☐ Organisational ☐ Compliance	

26. One of the principles of data protection is to process no more personal data than necessary. Is all information being processed by the project necessary?

Response	Risk type	Outcome
☒ Yes ☐ No If no, please detail ……	☐ Individual ☐ Organisational ☐ Compliance	

27. Has the Project Lead spoken to Service Management about updating the Service Catalogue to include the required Information Governance elements?

Response	Risk type	Outcome

☐Yes ☐No	☐ Individual ☐ Organisational ☐ Compliance	

Section C – IG Requirements Schedule [insert project name]

The requirements schedule forms part of Digital Health and Care Wales' Privacy Impact Assessment (PIA) process. This document must be read in conjunction with the project description for [insert project name] (section A)

Following the review of the populated PIA table (section B) the allocated IG lead and project lead/manager will agree the information governance / privacy requirements and record them on the IG requirements schedule. Each requirement will be scored against the risk matrix at Appendix 3. The requirements schedule will be used to capture progress against each requirement and note the final outcomes. It should be stated whether the risks identified have been eliminated, reduced or accepted.

The schedule is designed to be a living document which is updated regularly as the development progresses.

Using red, amber and green (RAG) as progress indicators within the schedule, by the time the project goes to the Wales Information Assurance Board (WIAB) for approval to go live all requirements should be green. However, dependent on the nature of the project and the issues raised it is possible that requirements may be amber or in an exceptional case even red; where this is the case the organisations involved must agree to accept any residual risk.

See Appendix 2 for further guidance on how to complete the requirements schedule.

Data Protection Impact Assessment Template

Ref	Question No.	Identified Requirement	Risk Assessment					Time-scale	Lead	Completion (RAG)	Comments / Progress / Further Action / Final Outcome
			Risk History	Likelihood	Impact	Score	Status (low, moderate, high, Extreme)				
RQ1			Initial								
			Residual								
RQ2			Initial								
			Residual								
RQ3			Initial								
			Residual								
RQ4			Initial								
			Residual								

Has all outstanding risks/requirements been copied to the programmes risks and issues log? ☐Yes ☐No
Are any residual risks scored higher than 10? ☐Yes ☐No
If Yes, has the ICO been consulted on the processing? ☐Yes ☐No
If the ICO has not been consulted on the processing and a residual risk is scored higher than 10, please state the reasons for not consulting the ICO below.

Appendix 1 – Risk Type

Risk Type – this is the 'classification' as noted on the PIA table (risk to individuals, compliance risk, organisation/corporate risk) and is noted in Section B

Risks to individuals	Compliance risk	Associated organisation/corporate risk
• Inadequate disclosure controls increase the likelihood of information being shared inappropriately. • The context in which information is used or disclosed can change over time, leading to it being used for different purposes without people's knowledge. • New surveillance methods may be an unjustified intrusion on their privacy. • Measures taken against individuals as a result of collecting information about them might be seen as intrusive. • The sharing and merging of datasets can allow organisations to collect a much wider set of information than individuals might expect. • Identifiers might be collected and linked which prevent people from using a service anonymously. • Vulnerable people may be particularly concerned about the risks of identification or the disclosure of information. • Collecting information and linking identifiers might mean that an organisation is no longer using information which is safely anonymised. • Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, presents a greater security risk. • If a retention period is not established information might be used for longer than necessary.	• Non-compliance with the common law duty of confidentiality • Non-compliance with the duties in the Health & Social Care (Safety & Quality) Act 2015 • Non-compliance with the relevant data protection legislation • Non-compliance with the Privacy and Electronic Communications Regulations (PECR). • Non-compliance with sector specific legislation or standards. • Non-compliance with human rights legislation.	• Non-compliance with the relevant data protection legislation or other legislation can lead to sanctions, fines and reputational damage. • Problems which are only identified after the project has launched are more likely to require expensive fixes. • The use of biometric information or potentially intrusive tracking technologies may cause increased concern and cause people to avoid engaging with the organisation. • Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, is less useful to the business. • Public distrust about how information is used can damage an organisation's reputation and lead to loss of business. • Data losses which damage individuals could lead to claims for compensation.

Appendix 2 - Additional Guidance notes for completion of the Requirement Schedule

- **Ref -** Unique number allocated to each requirement (RQ) within the schedule, the reference number should be noted against the relevant question in the PIA table.
- **Identified Requirement –** Details of the IG requirement identified and a brief description of the risk posed if the requirement is not addressed. The Risk Type, as identified in the PIA table should be
- **Risk History** – This is the status of the risk, whether it is the initial risk or the residual risk
- **Likelihood** – What is the likelihood of breaching the DPA/GDPR if no action is taken. This should be scored as per the table below.
- **Impact** – This is the severity of the impact of a breach of the DPA/GDPR if no action is taken. This should be scored as per the table below.
- **Score** – This is the likelihood score x the impact score.
- **Status** – This is whether the risk is low, medium, high or extreme. The score dictates the status as per the table below.
- **Timescale** – For each requirement to be addressed within, as aligned to the project timescales;
- **Lead** – Person responsible for taking each requirement forward;
- **Completion (RAG)** – The level of progress applicable to that action in red (for not begun), amber (in progress), green (complete)
- **Comments / Progress / Further Action / Final Outcome** describe the progress to date for each requirement (each entry should be dated), list any additional comments and further actions as appropriate. Ensure that it is noted if a risk has been eliminated, reduced or accepted. Any significant actions should be fed in as a further requirement.

Appendix 3 - Risk Scoring Tables

Likelihood score	1	2	3	4	5
Descriptor	**Rare**	**Unlikely**	**Possible**	**Likely**	**Almost certain**
Frequency How often might an IG breach occur	This will probably never happen/recur	Do not expect it to happen/recur but it is possible it may do so	Might happen or recur occasionally	Will probably happen/recur but it may not be a persisting issue	Will undoubtedly happen/recur, possibly frequently

Impact score (severity levels) and examples of descriptors	1	2	3	4	5
	Negligible	**Minor**	**Moderate**	**Major**	**Catastrophic**
Impact on an individual's privacy and confidentiality	Minimal privacy impact requiring no/minimal intervention Other manual or electronic process in place to mitigate the IG risk	Minor impact on an individual's privacy Other manual or electronic process in place to mitigate the IG risk	Moderate privacy impact requiring professional intervention Aspects of reputational damage for the organisation if IG requirement not adopted Could result in an event which impacts on a moderate (less than 100) number of patients/clients	Major breach leading to possible larger scale privacy breaches Mismanagement of patient/client privacy with long-term reputational issues Would impact on over 100 patients/clients – part system failure	Serious IG breach and non-compliance with the law if requirement not adhered to An event which impacts on a large number of patients/clients – full system breach because of no adherence to standards. Is likely to be 1000 of patients/clients

		Likelihood				
		1	2	3	4	5
		Rare	**Unlikely**	**Possible**	**Likely**	**Almost certain**
Impact Score	**5 Catastrophic**	5	10	15	20	25
	4 Major	4	8	12	16	20
	3 Moderate	3	6	9	12	15
	2 Minor	2	4	6	8	10
	1 Negligible	1	2	3	4	5

Status

	1 - 3	Low risk
	4 - 6	Moderate risk
	8 - 12	High risk
	15 - 25	Extreme risk