CURISTICA

HANLEY CONSULTING

Surgery Assist Data Protection Impact Assessment (DPIA)

Document Reference: 250314_SA_DPIA_V1.0

Version: 1.0

Date: 14/03/2025

Status: Published

Director: Sharon Hanley

Document Management

Revision History

Version	Date	Summary of Changes
1.0	14/03/2025	Published

Authors

Name	Title/Responsibility	Date	Version
Dr Youssof Oskrochi	Data Protection Officer (Curistica Ltd)	14/03/2025	1.0

Reviewers

This document must be reviewed by the following people:

Name	Title/Responsibility	Date	Version
Sharon Hanley	Director		
Dr Keith Grimes	Chief Digital Health Officer & CSO		

Approved by

This document must be approved by the following people:

Name	Title/Responsibility	Date	Version
Dr Youssof Oskrochi	Data Protection Officer (Curistica Ltd)	14/03/2025	1.0

Based on the NHS England Health and Social Care DPIA Template (Accessed 01/10/2024)

Table of contents

SECTION 1 – Screening

1. Do you need to do a DPIA?

a. Summary of how data will be used and shared

Surgery Assist systematically collects information in 2 ways.

1. Automatically through use of the service we collect technical and behavioural data from users interacting with our product. No directly personally identifiable data is collected.
2. User input as users are able to leave comments in free-text boxes for the purposes of feedback, bug identification or suggestions. In these instances they may, after providing explicit consent, also leave their contact details if they wish to be followed up.

For the purposes of this DPIA, we will only consider the automatic collection of data.

The collection of personal data through the feedback mechanisms, which require explicit consent of the user, has been assessed and deemed to be small-scale with limited processing, therefore not requiring a formal DPIA. Further rationale is provided in Appendix A.

b. Description of the data

☐	Personal data
☐	Pseudonymised data
☐	Anonymous data

SECTION 2 – Data purpose and use

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

The data collected is used for:

1. Monitoring the performance and usage of the digital assistant.
2. Improvement of the product by analysing user behaviour and identifying areas where the assistant's functionality can be enhanced.
3. Identification of faults and troubleshooting technical issues that may arise during user interactions.
4. Usage analytics to understand how often users engage with the assistant, which devices they use, and how long sessions last.
5. Enhancing user experience by using the insights to provide a more efficient and user-friendly service.

Data would be shared with the client (e.g. the GP practice) only on an aggregate level to inform them about the performance of the system.

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

1. Monitoring the performance and usage of the digital assistant helps ensure smooth functionality and consistent service delivery. This allows the product to operate reliably for users.
2. Improvement of the product by analysing user behaviour, which provides insights into how the assistant can be further enhanced. This leads to more intuitive features and a better user experience over time.
3. Identification of faults helps to detect and resolve technical issues quickly, ensuring minimal disruption for users and increasing system reliability.
4. Usage analytics give us a deeper understanding of user interaction patterns, such as which devices are most used, session durations, and frequent entry points. This enables better optimisation for different devices and more tailored user experiences.
5. Enhancing the user experience through continuous product refinement based on data-driven insights, ensuring the service is responsive to user needs and preferences

SECTION 3 – Data types, sources and linkage

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

☐	Yes
☐	No
☐	Unsure

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

☐	Forename	☐	Physical description, for example height	☐	Photograph / picture of people
☐	Surname	☐	Phone number	☐	Location data
☐	Address	☐	Email address	☐	Audio recordings
☐	Postcode full	☐	GP details	☐	Video recordings
☐	Postcode partial	☐	Legal representative name (personal representative)	☐	Other:
☐	Date of birth	☐	NHS number	☐	None
☐	Age	☐	National insurance number		
☐	Gender	☐	Other numerical identifier: ConversationID, UserID		

- **GP Details:** the ODS code for the practice is captured as Surgery Assist is implemented on a per-practice setting. This is integral to its functioning as Surgery Assist is tailored for each practice's unique demands.
- **Other Numerical identifier:**
    - **ConversationID**: Random conversationID allowing session metrics to be recorded.
    - **UserID:** Surgery Assist generates a unique UserID internally for each individual based on their IP address. This is only for identification of new vs returning users. If a returning user has the same IP address, the same UserID will be used.The UserID cannot be reverse engineered to the IP address.
- **Dataset structure:**

Data	Format	Collection Method	Who collects?	Who is it sent to?
Conversation ID	Numeric	Randomly generated	Microsoft Azure	Hanley Health Ltd
User ID	Numeric	Randomly generated	Microsoft Azure	Hanley Health Ltd
Returning/New User	Boolean	HTTP Header	Microsoft Azure	Hanley Health Ltd
Referrer URL	URL	HTTP Header	Microsoft Azure	Hanley Health Ltd
Operating System (iOS/Android/Linux/)	String	HTTP Header	Microsoft Azure	Hanley Health Ltd
ODS code	Alphanumeric	Chatbot used	Microsoft Azure	Hanley Health Ltd
Chat status (open/closed)	Boolean	By Model (Closed)	Microsoft Azure	Hanley Health Ltd
Chat started	date-time	API	Microsoft Azure	Hanley Health Ltd
Chat closed	date-time	API	Microsoft Azure	Hanley Health Ltd
Chat duration	date-time	Calculation	Microsoft Azure	Hanley Health Ltd
Chatbot Name	String	Chatbot used	Microsoft Azure	Hanley Health Ltd
Timestamp	date-time	Automatically generated	Microsoft Azure	Hanley Health Ltd

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?

Type of data		Reason why this is needed
☐	Information relating to an individual's physical or mental health or condition, for example information from health and care records	
☐	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	
☐	Racial or ethnic origin	
☐	Political opinions	
☐	Religious or philosophical beliefs	
☐	Trade union membership	
☐	Information relating to criminal or suspected criminal offences	
☐	**None of the above**	None of the data we routinely collect could be classified as special category data, nor could it conceivably be linked to special category data.

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

☐	Patients or service users
☐	Carers
☐	Staff:
☐	**Wider workforce:** whilst individual staff cannot be identified, the GP practice is identifiable and therefore the workforce at that practice may be (particularly if its a small practice).
☐	Visitors
☐	Members of the public
☐	Other:

8. Where will your data come from?

Data is collected from the interaction of service users with the Surgery Assist service.

9. Will you be linking any data together?

☐	Yes
☐	**No**
☐	Unsure

SECTION 4 – Data flows

10. Describe the flows of data.

Data flow name	Going from	Going to	Data description
Surgery Assist Usage Data IN	Microsoft Azure	Hanley Health Ltd	Raw data outlined in this DPIA received.
Surgery Assist Usage data OUT	Hanley Health Ltd	Primary Care Analytics	Data outlined in this DPIA sent for analysis.

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

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

☐	Yes
☐	No
☐	Unsure

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

SECTION 5 – Intended use and legal basis

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

☐	(a) We have consent
☐	(b) We have a contractual obligation
☐	(c) We have a legal obligation
☐	(e) We need it to perform a public task
☐	**(f) We have a legitimate interest - See attached LIA**
☐	Other:

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?

☐	(a) We need it to comply with our legal obligations for employment
☐	(b) We need it for legal claims, to seek legal advice or judicial acts
☐	(c) We need to comply with our legal obligations to provide information where there is a substantial public interest, as set out in this list
☐	(d) We need it to comply with our legal obligations to provide or manage health or social care services
☐	(e) We need it to comply with our legal obligations for public health
☐	(f) We need it for archiving, research and statistics where this is in the public interest
☐	Other
☐	**Not applicable**

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

☐	Implied consent
☐	Explicit consent
☐	Section 251 support
☐	Legal requirement
☐	Overriding public interest
☐	**Not applicable**

a. Please provide further information or evidence.

SECTION 6 – Data storage and security

16. Are you collecting information?

☐	**Yes**
☐	No

a. How is the data being collected?
Data is collected automatically by the platform (Microsoft Azure) during use by the end-user.

17. Are you storing information?

☐	**Yes**
☐	No

a. How will information be stored?

Storage location		**Details (leave blank if not applicable)**
☐	Physical storage, for example filing cabinets, archive rooms etc	
☐	Local organisation servers	
☐	**External organisation servers**	Data is stored on a secure Microsoft Azure Environment located in the UK. When downloaded, stored on secured Hanley Google Drive.
☐	Other	

18. Are you transferring information?

☐	**Yes**
☐	No

a. How will information be transferred?

Data flow name	Going from	Going to	Transfer Type	Frequency	Method
Surgery Assist Usage Data IN	Microsoft Azure	Hanley Health Ltd	Download	Monthly	Secure login
Surgery Assist Usage data OUT	Hanley Health Ltd	Primary Care Analytics	Email	Monthly	Secure package

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

Security measure		Details (leave blank if not applicable)
☒	**Encryption**	Microsoft Azure: AES 256 Google Drive: AES 256
☒	**Password protection**	
☒	**Role based access controls (RBAC)**	
☐	Restricted physical access	
☐	Business continuity plans	
☐	Security policies	
☒	**Other**	Multi Factor Authentication

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.

Security measure		Details (leave blank if not applicable)
☒	**Contract**	In place with all processors and clients
☐	Data processing agreement	
☒	**Data sharing agreement**	In place with all clients.
☐	Data sharing and processing agreement (DSPA)	
☐	Audit	
☐	Staff training	
☐	Other	

SECTION 7 – Data retention and deletion

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

We are currently using the data and will continue doing so throughout the lifecycle of the Surgery Assist platform.

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

7 years

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

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)**	Data processors (Microsoft Azure, Primary Care Analytics, Google Drive)

☐	Permanent preservation by transferring the data to a Place of Deposit run by the National Archives	
☐	Transfer to another organisation	
☐	Extension to retention period	
☐	It will be anonymised and kept	
☐	The controller(s) will manage as it is held by them	
☐	Other	

SECTION 8 – People's rights and choices

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

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 [Surgery Assist . We consider the communications methods below meet this obligation because of the nature of the interaction with the service, the expectation of the user with respect to the manner they would be informed and the necessity given the likely impact.
	☐	Privacy notice(s) for all relevant organisations - available on Privacy Policy - Hanley Health Ltd
	☐	Information leaflets
	☐	Posters
	☐	Letters
	☐	Emails
	☐	Texts
	☐	Social media campaign
	☐	DPIA published (best practice rather than requirement)
	☐	Other

	☐	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.	**N/A** - No personal information collected. Any information collected cannot be attributed to any identifiable individual either.	
The right to rectification The right to have inaccurate personal data rectified or completed if it is incomplete.	**N/A** - No personal information collected. Any information collected cannot be attributed to any identifiable individual either.	
The right to erasure The right to have personal data erased, if applicable.	**N/A** - No personal information collected. Any information collected cannot be attributed to any identifiable individual either..	
The right to restrict processing The right to limit how their data is used, if applicable.	**N/A** - Individuals may opt out by not using the service.	
The right to data portability The right to obtain and re-use their personal data, if applicable.	**N/A** -No personal information collected. Any information collected cannot be attributed to any identifiable individual either.	
The right to object The right to object to the use and sharing of personal data, if applicable.	**N/A** - No personal information collected. Any information collected cannot be attributed to any identifiable individual either.	

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

☐	Yes
☐	**No**
☐	Unsure

Explanation: No confidential personal information is being collected.

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

☐	Yes
☐	**No**
☐	Unsure

a. Where the effect of the automated decision on the individual is substantial, how will you uphold an individual's right not to be subjected to a decision solely made by automated means)?

b. Are you using any special category data as part of automated decision making?

☐	Yes
☐	**No**

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

None

SECTION 9 – Other organisations

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

Hanley Health Ltd

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

Processor	Role
Microsoft Azure	Collects and stores data on behalf of Hanley Health Ltd
Primary Care Analytics	Analyses data on behalf of Hanley Health Ltd
Google Drive	Stores data on behalf of Hanley Health Ltd

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

Not applicable - no subcontractors

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

See Question 29.

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

Due diligence measures		Details (leave blank if not applicable)
☐	**Data Security and Protection Toolkit (DSPT) compliance**	Microsoft: 8JH14 Google LLC: 8JE14 Primary Care Analytics: I4Z2B
☐	**Registered with the Information Commissioner's Office (ICO)**	Microsoft: Z6647359 Google LLC: Z6647359

☐	Digital Technology Assessment Criteria (DTAC) assessment	
☐	**Stated accreditations**	
☐	**Cyber Essentials or any other cyber security certification**	Microsoft: SOC1/2/3, Cyber Essentials Plus, G-Cloud, ISO 27001, 27017, 27018, 27701 Google: SOC1/2/3, Cyber Essentials Plus, Cloud Security, ISO 27001, ISO 27017, ISO 27018, ISO 27701
☐	Other checks	

SECTION 10 – Risks and Mitigations

33. Risk assessment table

Risk ref no.	Description	Initial risk score	Mitigations	Residual risk score
01	Loss of Surgery Assist Usage data	2	Regular backups by data processors (in-place already)	1
02	Inadvertent sharing of Surgery Assist usage data	2	Maintain security precautions, encryption and secure packaging of all data transfers (in place already)	1
03	Users not aware of systematic collection of data	4	All clients to be informed of and have clear signposting to privacy policies on their websites where Surgery Assist is being deployed.	2

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
3	Audit clients to ensure website privacy policies displayed and up to date	Sharon Hanley	Max Gattlin	15/01/2025	In progress

SECTION 11 – Review and sign-off

Reviewer sign-off	
Reviewer name:	Sharon Hanley
Reviewer job title:	Managing Director
Reviewer contact details:	sharon@hanleyconsulting.co.uk
Date of review:	14/03/2025
Comments:	Approved. Risk Ref 3 mitigation actioned.
Date for next review:	14/03/2026

Approver sign-off	
Approver name:	Youssof Oskrochi
Approver job title:	Data Protection Officer
Approver contact details:	youssof.oskrochi@curistica.com
Date of approval:	14/03/2025
Comments:	Approved

Appendix A

Rationale for Feedback collection not requiring a full DPIA.

Surgery Assist is a digital assistant for primary care that supports patients to self-serve and carry out administrative activities by signposting individuals to available online services, websites and apps.

The platform does not routinely collect, process or store any personally identifiable data during normal operation and users are generally unable to enter personal data through normal use of the Surgery Assist platform.

The Surgery Assist feedback function is therefore not deemed to require a full DPIA as we do not undertake processing which likely results in high risk to the rights and freedoms of individuals under UK GDPR or under European Guidelines.

Surgery Assist is also not operating as an innovative technology under the ICO's definition and is not collecting novel forms of data.

The only scenario where user personal data may be left is if users inadvertently leave PII or special category data (health) when entering information on the feedback form through a misunderstanding of the purpose of the form.

To mitigate this there are clear notices when using the forms and formal assessment is made within our Clinical Safety Hazard Log.

Users may however choose to leave their contact details (and must explicitly consent to this) if they wish to be contacted by us to go through their feedback with them.

To date, we have no recorded instance of any inadvertent submission of PII or health data via our feedback mechanisms. This is in the context of Surgery Assist recording over 174,000 interactions with clients and receiving 294 individual feedback submissions through our platform.

In summary, the platform is not designed for and we do not collect any personal data routinely. Any personal data collected is either consented or inadvertent, the latter which we have mitigated as best we can. Therefore any unintended data collection or processing of PII or special category data will be small-scale by nature.

This therefore does not constitute a "high risk" to the rights and freedoms of individuals, negating the need for a DPIA.