DPIA - Omni Consultation

DOCUMENT

Document Status	Live
Document Author	Daniel Grainge
Issue Date	28th October 2025
Next Review Date	28th October 2026

REVISION HISTORY

Version	Summary of Changes	Date
1.0	Document created	26 Oct 2025

AUTHORS

Version	Name	Title/Responsibility	Date
1.0	Daniel Grainge	Product Assurance Officer	26 Oct 2025

REVIEWERS

Version	Name	Title/Responsibility	Date
1.0	Richard Newell	DPO	27 Oct 2025

This is a controlled document. Whilst this document may be printed or downloaded as a PDF, this electronic version is the controlled copy. Any printed or PDF copies of the document are not controlled.

Section 1 - DPIA Requirement Assessment

X-on Health's Omni Consultation feature runs in parallel with the first iteration of a Voice Agent. The consultation form data can be gathered not just from the Voice Agent, but also via a Web Form and manual entry by staff, presenting an effective omnichannel approach.

A DPIA is needed for this feature, for the following reasons:

- X-on Health will be processing data which is sensitive (special category data). This includes identifiable health and care data.
- X-on Health will be implementing a new technology into Surgery Connect (Omni Consultation).

Section 2 - Processing Description

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or another way of describing data flows. What types of processing identified as likely high risk are involved?
The Omni Consultation feature involves the following processing activities: **Patient Identification & Verification:** Patients will identify themselves using a combination of personal data (e.g., Patient name, date of birth, and phone number) for both the Voice Agent and other Omni Consultation form channels.

Retrieval & Submission of Omni Consultation Details and Patient Action:

Voice Agent: Once the patient is identified via the Assign Patient Block in X-Flow, the patient progresses through to the Voice Agent Block which will then go through the Voice Agent Script (Consultation form). The Voice Agent repeats the patient response after each recorded answer, gaining confirmation that the recorded patient response is correct. For example, the Voice Agent will ask “Please describe the medical problem you’re calling about today”, and follows this up after listening to the response with “I’ve recorded that you’re calling about (described problem). Is that correct”.

Web form: Once the patient has navigated past the Web form landing page, pre-form warning (confirming this is not an emergency), whether the form relates to themselves or someone else, and confirming their details, they can then complete the Main Form page, answering the same consultation form questions across the omni channels.

Manual entry by staff**:** A blank consultation form is available for staff to complete manually, on behalf of the patient, during a call or face to face interaction. This ensures every patient’s needs are captured in the same structured way.

Post-Submission of Omni Consultation Form (All Channels)

Once the Omni Consultation form has been submitted, in all instances the data will land in a new Forms tab within the Communication Window of the Surgery Connect Phonebar, allowing designated staff to easily process, assign, set priorities/severities, and add comments to every response, effectively managing the entire triage workflow.

Managing Omni Consultation Form Data

Within the Service Delivery Console, users with the feature administrator privilege, can view historic form data within the retention period configured by the GP practice. These users will be able to re-open a previously closed response at the bottom right of the Closed tab in the Forms area, providing the retention period settings. The default retention for consultation form data within the X-on platform is 1 month, after which data is automatically and permanently deleted. Retention aligns with the NHS Records Management Code of Practice (2023) and the contractual data processing agreement between X-on Health and the Controller.

Other Processing Information

Data is not shared outside the scope of any Surgery Connect/X-on contracts.

Where Surgeries have integration with a clinical system such as EMIS (Optum) or SystmOne, connection is made between Surgery Connect and the clinical system, via the clinical systems secure API to identify the patient's information and functionality to write back to the patient's record. No associated patient data is stored on Surgery Connect and remains under the domain of the clinical system. Where the clinical system is inactive and or the user is signed out, Surgery Connect/the Phonebar will not show any patient information and requires full integration to work.

All call recording data is permanently deleted by internal processing after agreed retention periods.

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

Data Subjects - Patients with scheduled appointments within the specific GP practice can access this feature, turning the feature on is controlled by the practices themselves and they have complete control over the slots that can be checked & or Cancelled.

Data Categories - Personal Data: Name, contact details (phone number), date of birth

Special Category Data (Health Data) - Consultation details which may implicitly or explicitly reveal information about the patient's health (e.g., condition details like "sugar levels are low", type of appointment requested, clinician speciality).

Data Storage - Consultation data is primarily stored in existing clinical systems. The Omni Consultation form and Voice Agent features will interact with these systems. Temporary data logs related to the transaction (e.g., access logs, cancellation requests) will be created and stored by the reporting platform for audit.

Data Sharing:

Internally - Between the Omni Consultation and Voice Agent feature and the organisation's clinical systems. Relevant staff will see updated Consultation form statuses in the Forms area.

Externally - Data will be processed by X-on Health acting as a Data Processor.

Geographical Area of Processing - UK data centres.

Detail Retention and Deletion - It is the practices' role to, when required, inform the patient of how long their data is retained and at what point it is deleted.

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

X-on has no relationship with individual callers. X-on acts as a data processor in relation to any personal data for and on behalf of the Surgery Connect customer, who remains the data controller in relation to such personal data.

This feature is being implemented to:

- Gathers clear, structured, and complete consultation form responses, significantly reducing the need for costly and time-consuming doctor call backs.
- Automates the initial, high volume task of consultation form data gathering, freeing up reception and clinical teams for direct patient care, reducing staff burnout.
- Provide an efficient and omni channel way for patients to contact their GP Surgery and request a consultation/appointment. Improving patient convenience, access, and experience.

X-on is ISO 27001, ISO9001, ISO14001, ISO22301 & ISO 42001 certified and holds Cyber Essentials Plus.

All data is securely held in UK data centres under the control of X-on as governed by the NHS DSP (Data Security & Protection) regulations, &

completes the NHS DSP Toolkit (DSPT) - exceeding the national standards. X-on is an approved supplier.

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing for you, and more broadly?

The purpose of processing personal data via this feature is to:

- To collect and structure patient information for patient triage, ensuring consistency and equity in how patient needs are captured, regardless of the omni channel used (Voice Agent, Web Form, or Manual Entry by Staff).
- To enable practice staff to process and manage patient requests by providing a unified view of all consultation data in a central location. This includes the ability to assign, prioritise, and comment on each response.
- To facilitate communication and workflow by creating a new tab within the Communications Window where designated staff can easily access and process consultation responses from all channels, thereby streamlining the entire triage process.

Section 3 - Consultation Process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

X-on Health acts as a data processor and has no relationship with individual callers so seeking their views is not appropriate.

The responsibility for monitoring data protection compliance within the organisation rests with the Data Protection Officer. It is the responsibility of X-on Health's Network Team to provide adequate protection and confidentiality of all corporate data and proprietary software systems, whether held centrally, on local storage media, or remotely, to ensure the continued availability of data and programs to all authorised members of staff, and to ensure the integrity of all data and configuration controls.

Section 4 - Assessment of Necessity and Proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?
Processing is necessary for the performance of a contract with our Surgery Connect customers (UK-GDPR Article 6.1(b) for this lawful basis of processing). X-on acts as a data processor for and on behalf of the Surgery Connect customer, who remains the data controller in relation to such personal data with responsibility for communication with individuals. **The processing is necessary to:** • Provide a modern, accessible method for patients to manage appointments. • Address the operational and financial impact of DNAs (did not attends). • Empower patients with more control over their healthcare appointments. • Alternative methods (e.g., phone calls) can be less efficient, more resource-intensive, and less convenient for patients. **Proportionality:** The amount and type of data processed are limited to what is necessary to achieve the stated purposes. Patient verification methods are designed to be robust enough to confirm identity without being overly intrusive. If the patient is not an exact match within the clinical system, they are not able to use this service/feature. Only relevant appointment details are displayed & controlled by the practice. The benefits of the feature (reduced DNAs, improved patient experience, efficiency) are considered to outweigh the potential privacy risks, provided appropriate safeguards are in place.

Step 5: Identify and assess risks

Describe the source of risk and nature of potential impact on individuals. Include associated	**Likelihood of Harm** (Remote,	**Severity of Harm** (Minimal,	**Overal l Risk**

compliance and corporate risks as necessary.	Possible or Probable)	Significant or Severe)	(Low, Medium or High)
Omni Consultation forms accessed by an unknown third party	Remote. Our system and network security should stop this.	Significant - If form holds sensitive data could be a GDPR data breach.	Low
Omni Consultation forms accessed by an unauthorised user	Possible. If customer data controls are weak	Significant - If form holds sensitive data could be a GDPR data breach.	Medium
Patient Misidentification	Possible.	Significant - Could result in confidentiality breach.	Medium
Human error with Manual Entry by Staff consultation form	Possible.	Significant - Could result in inaccurate data.	Medium

Step 6: Lawful Basis for Processing

As the processing may include the process of Special Category Patient Data - we must include the lawful basis for processing such data under the current legislation (UK GDPR) - Likely basis: **9(2)(h) - provision of health or social care**. The **GP practice (controller)** must base their processing on **Article 6(1)(e) – task in the public interest**.

Step 7: Identify and assess risks

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5:				
Risk	**Options to Reduce or Eliminate Risk**	**Effect on Risk** (Remote, Possible or Probable)	**Residual Risk** (Minimal, Significant or Severe)	**Measure Approved** (Low, Medium or High)
Omni Consultation forms accessed by an unauthorised user	• Three levels of access control available relating to Omni Consultation form access. • Clinical System Integration required to view patient information. Secure SSO.	Remote	Minimal	Low
Patient Misidentification	• Multi-factor identity verification (DOB, Name, Telephone number) • Regularly test identity verification logic using test data sets • Multiple Failsafe Windows in the Phonebar	Remote	Minimal	Low
Human error with Manual Entry by Staff	• Clinician's mandatory review and standard GP	Remote	Minimal	Low

consultation form	triage process highlighting errors. • Audit trails • Mandatory fields			

Step 8: Sign off and record outcomes

Sign Off Task	Name/date	Notes
Measures approved by	Melissa Lato	
Residual risks approved by	Melissa Lato	
DPO advice provided	Richard Newell	
Summary of DPO advice - N/A		
DPO advice accepted or overruled by	Daniel Grainge / Melissa Lato	
Comments: N/A		
Consultation responses reviewed by	Daniel Grainge	
Comments: N/A		
This DPIA will be kept under review by	Daniel Grainge	The DPO should also review ongoing compliance with DPIA.