DPIA - Surgery Connect

DOCUMENT

Document Status	Live
Document Author	X-on Health DPO
Issue Date	2 Oct 2025
Next Review Date	2 Oct 2026

HISTORY

Version	Amendment	By	Date
2.0	New document replacing version 1.4	Richard Newell, DPO	2 Oct 2025
2.1	Added Google as a sub-processor	SH & NM	1 Dec 2025
2.1	Added Cloudflare as a sub-processor	SH & NM	12 Feb 2026
2.1	Added Hubspot and Datto Autotask as sub-processors; Teamviewer and Firetext	SH & NM	2 Mar 2026
2.2	Added Video Call details	DG	27 Mar 2026

Step 1: Identify the need for a DPIA

Explain broadly what the project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Complete the checklist to assess whether a DPIA is required.

Required	Details
The project is designing a product that will: *(tick all those that apply)*	
	Use systematic and extensive profiling or automated decision-making to make significant decisions about people.
☑	Process special category data or criminal offence data on a large scale.
	Systematically monitor a publicly accessible place on a large scale.
☑	Use new technologies.
	Use profiling, automated decision-making or special category data to help make decisions on someone's access to a

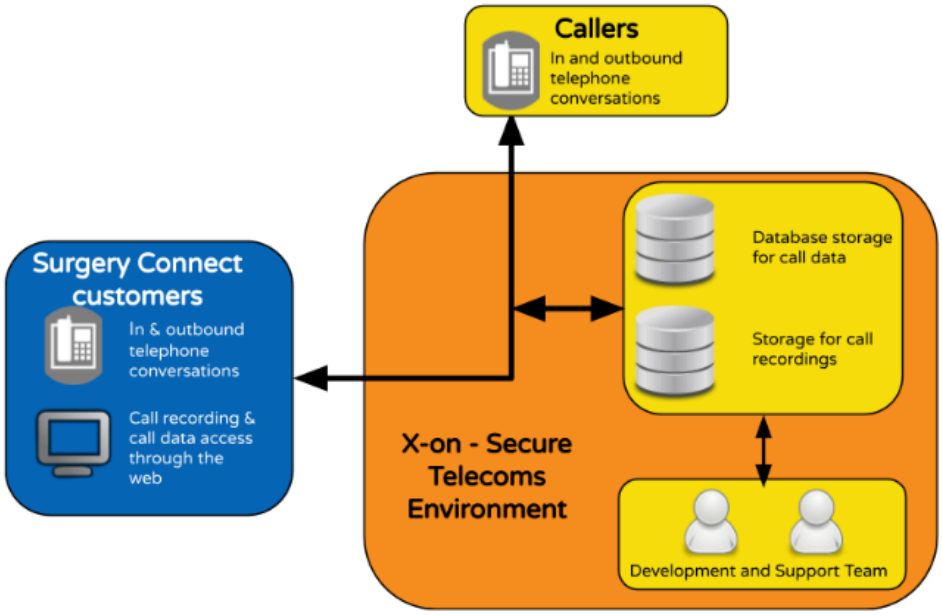
	service, opportunity or benefit.
	Carry out profiling on a large scale.
	Process biometric or genetic data.
	Combine, compare or match data from multiple sources.
☑	Process personal data without providing a privacy notice directly to the individual.
	Process personal data in a way which involves tracking individuals' online or offline location or behaviour.
	Process children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them.
	Process personal data which could result in a risk of physical harm in the event of a security breach.
We consider carrying out a DPIA if we plan to carry out any other: *(tick all those that apply)*	
	Evaluation or scoring.
	Automated decision-making with significant effects.
	Systematic.
☑	Processing of sensitive data or data of a highly personal nature.
	Processing on a large scale.
☑	Processing of data concerning vulnerable data subjects.
	Innovative technological or organisational solutions.
	Processing involving preventing data subjects from exercising a right or using a service or contract.

Step 2: Describe the processing

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?

Surgery Connect is a telephony system and as such processes call data records between callers and our customer health organisations

The diagram below shows data flows. Surgery Connect customers access the data through user consoles.



Data is not shared outside the scope of Surgery Connect contracts.

The call data records contain telephone numbers which are considered under GDPR as non-sensitive personal identifiers and for Surgery Connect there is no association with patient names or other personal identifiers. Telephone numbers however are subject to the highest security controls.

Where surgeries have integration with a clinical system such as EMIS, connection is made via the clinical systems secure API by passing the telephone number to identify the patient's record. No associated patient data is stored on Surgery Connect and remains under the domain of the clinical system.

[Phone call data is processed in the normal way during surgery connect processing. The EMIS integration receives an event on the local client PC to indicate that a phone call has started.

The application does a local EMIS lookup to get non clinical patient data - name, date of birth, patient ID. The name and date of birth stays locally within the application on the PC.

The patient ID is transmitted back to x-on to be stored against the phone call record as a log of phone calls related to that patient.

SMS - the local application can also send SMS to the active patient. This involved the patient's mobile number and SMS message content being submitted to us to deliver the SMS. This is again logged against the patient ID.

Patient ID is not considered a personal identifier in the context of personal information as it is not of any use except if you have access to the heavily secure EMIS application at the doctors surgery.]

For surgeries that choose not to record calls, call records are kept for the contracted data retention period. Call records are retained for a minimum of 12 months in accordance with the absolute minimum specified to meet the NHS contractual requirement.

Where a user account record with associated call records has been deleted, either logically or physically, the call recordings may no longer be visible or accessible from the user interface. The associated call records remain in the secure file storage for the defined retention period.

Call recordings have the potential to contain sensitive health data including data from vulnerable data subjects and are subject to the strictest security controls. The processing per se is not considered high risk.

Data is retained in accordance with the contractually agreed retention period, most commonly 36 months. The 36 month call retention period complies with the NHS standard data retention period for calls not part of health records in line with Records Management Code of Practice (Aug 2021, updated Aug 2023) data retention schedules. The code of practice advises the transfer of any relevant information from call recordings into the main health record through transcription or summarisation. Call handlers may perform this task as part of the call for surgeries that have the clinical system integration such as EMIS. Where it is not possible to transfer clinical information from the recording to the

health record the recording must be considered as part of the record and be retained accordingly.

How the individual customers transfer any data they consider to constitute part of the patient's record to their health record is outside of the scope and under the control of the individual surgery. Call recordings can be downloaded by surgeries to their secure data stores outside of the control of Surgery Connect.

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

Practices recording patient calls have an IVR which informs the caller that the calls are recorded for monitoring and training purposes. Practices also have the option to not record any calls (no need for the IVR in this case) or can pause recording at any point during a conversation.

Call data records are subject to Ofcom regulated retention periods.

Nature of the Video Call Feature:
Surgery Connect provides an integrated Video Call service, utilising Whereby as a sub-processor, to facilitate web-based video consultations.

Collection and Use: Clinicians initiate a video call by sending a unique, one-time link to the patient via SMS directly from the Surgery Connect interface.

Source of Data: The video and audio streams are generated in real-time between the clinician’s and patient’s browser-enabled devices.

Infrastructure: The service is browser-based, meaning no patient data is stored via local application downloads on the user's device. Whereby does not store any data relating to the patient or the user.

Data Flows: Whereby prioritises peer-to-peer (P2P) connections where possible, meaning the video/audio data travels directly between the two devices without being stored by X-on. If network restrictions prevent P2P, the encrypted data is relayed through secure servers but is not recorded unless specifically configured by the surgery

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?
Surgery Connect processes call data records between patients and health organisations. The call data records contain telephone numbers which can be considered non-sensitive personal identifiers. Call recordings have the potential to contain sensitive health data including data from vulnerable data subjects. The data is operational and the system is active 24x7. Projected figures suggest up to 100 million call records will be processed per annum. The number of single callers cannot be sensibly estimated. Most callers and all health providers will be UK based. Data is retained in accordance with the contractually agreed retention period, most commonly 36 months. All data is permanently deleted by internal processing after agreed retention periods.
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. Voice over IP (VoIP) technology is well proven. X-on is ISO 27001 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. 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?
Surgery Connect provides a telephone system for Surgery Connect customers. X-on makes the data available to the customer. The benefit to X-on is commercial gain through providing the system to the customer and X-on has no further interest in the data processed.

Step 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 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'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. Although X-on has no direct relationship with patients, the ICO recommends considering proportionate consultation with stakeholders. For this service, that could include feedback from GP surgeries as controllers, representative patient groups, or professional bodies. External consultation has not yet been undertaken, but X-on will keep this under review, particularly if the scope of processing expands or new risks are identified.

Step 4: Assess 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?

X-on as Data Processor

X-on processes personal data strictly for the performance of a contract with Surgery Connect
customers (Article 6(1)(b) UK GDPR). X-on has no independent purpose for processing
patient data and acts only under the documented instructions of its healthcare customers.

GP Surgeries as Data Controllers

For patient-related processing, the controller's lawful basis differs:

Article 6(1)(e) – Public Task: Processing is necessary for the performance of a task carried
out in the public interest, namely the delivery of NHS healthcare services.

Article 6(1)(c) – Legal Obligation: In some cases, processing may also be required to meet
statutory or contractual NHS obligations.

Special Category Data

Call recordings may include health information that falls under special category data. The
appropriate lawful basis under Article 9 UK GDPR is:

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 the management of
health or social care systems and services.

Accordingly, while X-on as processor relies on Article 6(1)(b) (contract), controllers (GP
surgeries) rely on Article 6(1)(e) together with Article 9(2)(h) to lawfully

process any health-
related content captured in calls.

Supporting Data Subject Rights
As controllers, GP surgeries remain responsible for enabling patients to exercise their UK
GDPR rights, including:

Right of access – patients may request a copy of call recordings or associated call data.

Right to rectification – corrections to inaccurate personal data can be applied within the
underlying patient record; call logs can be annotated where appropriate.

Right to erasure – requests must be assessed by the controller in line with NHS retention
rules; where granted, X-on will act on the surgery's instructions to delete relevant records
from Surgery Connect systems.

Right to restriction and objection – patients may ask that call recordings not be retained or
used beyond necessary purposes. Surgeries can configure Surgery Connect (e.g. pausing
recording) to respect these preferences.

Right to data portability – unlikely to be relevant, but where applicable, data can be exported
in a machine-readable format upon the controller's request.

X-on as Processor
X-on will:

Provide the technical means for controllers to search, retrieve, export, and delete call
data/recordings.

Act promptly on any data subject rights request passed to it by the controller, in accordance
with the contract and Article 28 UK GDPR obligations.

Ensure all actions are logged and auditable.

This approach ensures that surgeries, as controllers, can fulfil their legal duties under
Articles 12–23 of the UK GDPR, with X-on providing full technical and contractual support.

There are no International Transfers as all processing is carried out within the UK.

Article 28 of the UK GDPR requires controllers (GP Practices) to have binding contracts with
processors. All GP surgeries using Surgery Connect have a signed Data Processing
Agreement with X-on. This sets out:

- subject matter and duration of processing
- nature and purpose of processing
- types of personal data and categories of data subjects
- obligations and rights of the controller

The contract also confirms X-on's duties on confidentiality, security, breach notification, sub-
processor management, audit rights, and assistance with data subject rights.

Transparency and Patient Information
Call Recording (IVR)
Patients are informed that calls may be recorded through the IVR message at the start of
each call. This provides a basic level of transparency about monitoring and training purposes.

SMS Communications
Where the Surgery Connect, application is used to send SMS messages to patients (e.g.
appointment reminders or follow-up instructions), transparency requirements under Articles
12–14 of the UK GDPR also apply.

- Patients telephone number and SMS content are processed by X-on as processor

- Their messages may be logged against a patient ID within Surgery Connect
- Retention and deletion of SMS data follows the same contractual terms as call records

Controllers (the GP surgeries) should ensure their privacy notices explicitly state that SMS
is used as a communication channel, what personal data is processed, and that processing
is carried out through X-on as a processor.

Video Call

Data Minimisation: The video consultation does not require or process any patient demographic information (like names or dates of birth) to initiate the call; it relies on a unique session URL and the patient's mobile number for the SMS invite.

Recording Controls: Video calls cannot be recorded.

Retention: Any video metadata (e.g. timestamp within Surgery Connect that a video call SMS invite has been sent to a patient) follows the contractually agreed retention period, typically 36 months, before being permanently deleted.

Who is Processing the Data
Patients should be made aware that:

- Their GP surgery remains the data controller responsible for the processing of call and SMS data
- X-on provides the Surgery Connect platform as a data processor under contract
- All data is securely hosted within UK data centres and subject to NHS DSP and ICO recognised safeguards

It is recommended that:

- Surgeries should update their local patient privacy notices to reference the use of Surgery Connect for calls and SMS
- Notices should specify the categories of data processed (phone numbers, call content, SMS content), the purposes (healthcare

communication, call handling), and the lawful bases (Articles 6 and 9 UK GDPR)

- Where SMS is used an initial message template could include a brief privacy reminder (e.g. “Your GP surgery uses a secure NHS-approved service to send this message. See our privacy notice [link]”

This ensures patients are consistently and clearly informed across all communication
channels, not just at the point of call recording.

Step 5: Identify and assess risks

Describe the source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm** (Remote, possible or probable)	**Severity of harm** (Minimal, significant or severe)	**Overall risk** (Low, medium or high)
Telephone number access by an unknown third party.	Remote. Our system and network security should stop this	Minimal - It’s just a phone number with no context around it	Low
Call recordings accessed by an unknown third party	Remote. Our system and network security should stop this	Significant - If record holds sensitive data could be a GDPR data breach	Low
Call recordings accessed by unauthorised user	Possible. If customer data controls are weak	Significant - If record holds sensitive data could be a GDPR data breach	Medium

Photos accessed by unauthorised user	Unlikely due to security controls in place and encrypted/anonymised data	Significant	Low
Sub-processor AWS fails to protect text to speech data so data is lost	Remote - AWS is under contract with X-on and operates at the very highest levels of security see AWS Customer Agreement	Significant harm to patient if it contains sensitive information could be a GDPR data breach	Low
Unauthorised access to video session: An unknown third party attempting to join a private clinical consultation.	Remote: URLs are unique and complex; clinicians have the option to pause or end sessions at any point	Significant: Potential exposure of sensitive health data.	Low
Sub-processor (Whereby) failure: Whereby fails to protect data streams or encounters a security breach.	Remote: Whereby operates under contract with X-on and is subject to the same high security standards as other sub-processors like Google or AWS.	Significant: Could lead to a GDPR data breach if sensitive info is exposed.	Low

Sub-processor Cloudflare fails in WAF and DDOS protection	Remote - Cloudflare operates at very high levels of security holding ISO27701	Significant harm possible, user interaction potentially exposed	Low
Sub-processor Google fails to protect data from loss	Remote - Google is under contract with X-on and operates at the very highest levels of security see Google Customer Agreement	Significant harm to patient if it contains sensitive information could be a GDPR data breach	Low
Sub-processor Hubspot fails to protect data from loss	Remote - Hubspot is under contract with X-on and operates at the very highest levels of security, holding SOC2	Minimal harm to customer information, no patient data is stored	Low
Sub-processor Datto Autotask fails to protect data from loss	Remote - Autotask is under contract with X-on and operates at the very highest levels of security, holding SOC2	Minimal harm to customer information, no patient data is stored	Low
Intercom powers X-on's Customer Chat function and Help Centre	Remote - Intercom operate at the very highest levels of	Minimal harm to customer information, patent data is	Low

	security holding ISO27001, SOC 2 & ISO42001	not relevant as it's a customer support chat and centre for the customer only	
Teamviewer provides remote access to customer PC's	Remote - this function is only used by X-on's Customer Support team for when a user needs more direct assistance.	Minimal harm, live help, nothing is stored or saved	Low
Firetext provides Practice to Patient text messaging	Remote - practice function for contacting patients	Minimal - and clinical information should not be sent by SMS	Low
SMS sent to wrong user	Remote - no different to normal human error of typing an incorrect number	Minimal - and clinical information should not be sent by SMS	Low

Step 6: Identify measures to reduce risk

In line with Article 25 of the UK GDPR, Surgery Connect has been developed according to "data protection by design and by default" principles. This includes:

- **Data minimisation** - only telephone numbers, call metadata, and optional recordings are processed; no unnecessary personal identifiers are stored
- **Access control by default** - user accounts are provisioned with least-privilege settings; access to recordings is logged and monitored
- **Logging and monitoring** - all access to call data and recordings is auditable, with alerts on unusual activity

- **Retention by default** - data is deleted after contractual retention periods with no “silent” extensions

These principles underpin the specific risk-reduction measures described below.

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)
Call recordings accessed by unauthorised user	Include instant staff management in the design of the secure, browser based user console that gives access to call recordings. Include: ● visibility of staff’s current status ● management of staff’s group membership ● remote management ● see individual call queue and talk durations	Reduced	Medium	Yes
Call recordings	Recordings stored independently from	Reduced	Low	Yes

are deleted when user record is deleted	user records			
Connectivity to data centres fail and data is lost	There are four data centres in different UK locations. Automatic failover will occur in the event that connectivity fails	Reduced	Low	Yes

Step 7: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by:	Derrick Measham	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	N/A	If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:	Richard Newell	DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice: Residual risks identified in this DPIA are currently low or medium. Where any future assessment concludes that a high residual risk remains after mitigation, X-on and the relevant data controller will follow a clear escalation path: • Seek additional technical or organisational controls		

- Where high risk cannot be reduces, the controller will consult the ICO before commencing or continuing processing, in ligh with Article 36 UK CGPR
- This decision tree approach ensures compliance with the ICO's expecation for risk escalation and consultation

The coverage of this impact assessment is appropriate and covers all relevant data processing and storage activities at X-on. The measures in place identify and mitigate risk to the fullest extent possible.

Additionally it should be noted that responsibility for maintaining user authorisations is largely handed over to the service operators through the web consoles provided, where remote assistance is provided by X-on support staff on request from authorised account operators, subject to protocol.

DPO advice accepted or overruled by:	DPO	If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:	n/a	If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will be kept under review by:	Richard Newell/Neil Miles	The DPO should also review ongoing compliance with DPIA