

DPIA - Surgery Connect

DOCUMENT

Document Status	Live
Document Author	Derrick Measham
Issue Date	20/11/2020
Next Review Date	28/11/2025

HISTORY

Version	Amendment	By	Date
1.0	Document created	LB	20/11/2020
1.1	Annual review - no changes	LB	29/11/2021
1.2	Annual review - no changes	LB	18/11/2022
1.3	Annual review - no changes	Derrick Measham	02/11/2023
1.4	Annual review - no changes	Derrick Measham	28/11/2024

i 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.

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: <i>(tick all those that apply)</i>	
	Use systematic and extensive profiling or automated decision-making to make significant decisions about people.
<input checked="" type="checkbox"/>	Process special category data or criminal offence data on a large scale.
	Systematically monitor a publicly accessible place on a large scale.
<input checked="" type="checkbox"/>	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.
<input checked="" type="checkbox"/>	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: <i>(tick all those that apply)</i>	
	Evaluation or scoring.
	Automated decision-making with significant effects.
	Systematic.
<input checked="" type="checkbox"/>	Processing of sensitive data or data of a highly personal nature.
	Processing on a large scale.

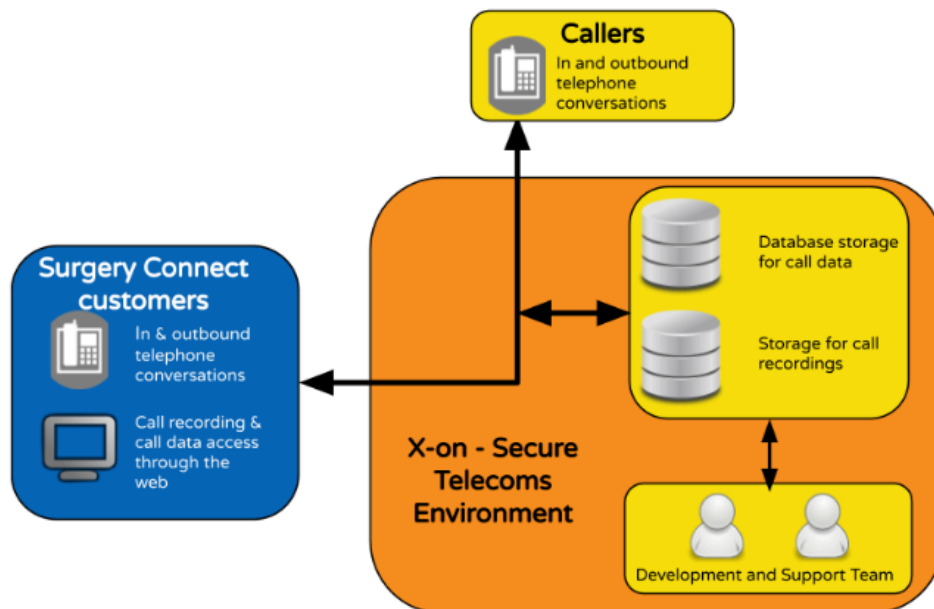
✓	Processing of data concerning vulnerable data subjects.
	Innovative technological or organisational solutions.
	Processing involving preventing data subjects from exercising a right or using a service or contract.

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 

[s 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.

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.

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?

Processing is necessary for the performance of a contract with our Surgery Connect customers. X-on acts as a data processor for and on behalf of the SurgeryConnect customer, who remains the data controller in relation to such personal data with responsibility for communication with individuals.

There are no international transfers.

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 photograph 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
SMS sent to wrong user	Remote or 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

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	<p>Include instant staff management in the design of the secure, browser based user console that gives access to call recordings.</p> <p>Include:</p> <ul style="list-style-type: none"> • 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 are deleted when user record is deleted	Recordings stored independently from user records	Reduced	Low	Yes
Connectivity to data centres fail and data is lost	<p>There are four data centres in different UK locations.</p> <p>Automatic failover will occur in the event that connectivity fails</p>	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:	CG	DPO should advise on compliance, step 6 measures and whether processing can proceed

Summary of DPO advice:

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:

LB

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:

Derrick Measham

The DPO should also review ongoing compliance with DPIA