NHS
Buckinghamshire, Oxfordshire and Berkshire West
Integrated Care Board

Data Protection Impact Assessment (DPIA) Template

A DPIA is designed to describe your processing and to help manage any potential harm to individuals' in the use of their information. DPIAs are also important tools for demonstrating accountability, as they help you as a Controller to comply with the requirements of the Data Protection Legislation. Non-compliance with DPIA requirements can lead to fines imposed by the Information Commissioners Office (ICO); this includes not carrying out a DPIA at all, carrying out a DPIA in an incorrect way or failing to consult the ICO where required.

DPIA's are not new; the use of Privacy Impact Assessments has become common practice in the NHS and can provide evidence of compliance within the Data Security and Protection toolkit (DSPT); DPIAs build on that practice.

It is not always clear whether you should do a DPIA or not but there are a number of situations where a DPIA **should** be considered or where a DPIA is a **legal requirement**. If you can tick against the criteria below it is highly recommended that you undertake a DPIA and if you decide not to, ensure that you document the reasons for your decision.

You as Controller **MUST** carry out a DPIA where you plan to:	Tick or leave blank
Use **profiling or automated decision-making** to make significant decisions about people or their access to a service, opportunity or benefit;	☐
Process **special-category data or criminal-offence data on a large scale**;	✓
Monitor a publicly accessible place on a large scale;	☐
Use **innovative technology** in combination with any of the criteria in the European guidelines;	✓
Carry out **profiling** on a large scale;	☐
Process biometric or genetic data in combination with any of the criteria in the European guidelines;	☐
Combine, compare or match data from multiple sources;	☐
Process personal data **without providing a privacy notice** directly to the individual in combination with any of the criteria in the European guidelines;	☐
Process personal data in a way that involves **tracking** individuals' online or offline location or behaviour, in combination with any of the criteria in the European guidelines;	☐
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 that could result in a **risk of physical harm** in the event of a security breach.	☐

You as Controller should **consider** carrying out a DPIA where you	Tick or leave blank
Plan any major project involving the use of personal data;	✓
Plan to do evaluation or scoring;	☐
Want to use systematic monitoring;	☐
Process sensitive data or data of a highly personal nature;	✓
Processing data on a large scale;	☐
Include data concerning vulnerable data subjects;	✓
Plan to use innovative technological or organisational solutions;	✓

A new DPIA should be carried out if you decide that there is a significant enough change to what you originally intended but it is good practice for DPIAs to be kept under review and revisited when necessary.

There is guidance to help you. Your Data Protection Officer (DPO) can be consulted before completing a DPIA in order to provide specialist advice and guidance or simply to talk things through with you.

Background Information	
Date of your DPIA :	22/04/2024
Title of the activity/processing:	Silicon Practice (Footfall)
Who is the person leading this work?	[redacted]
Who is the Lead Organisation?	BOB ICB
Who has prepared this DPIA?	[redacted]
Who is your Data Protection Officer (DPO)?	[redacted]
Describe what you are proposing to do: (Include as much background information as you can about why the new system/change in system/sharing of information/data processing is required).	Silicon Practice provides an Online Consultation (OC) solution that is integrated to the Footfall Practice website for GP Surgeries. They allow patients to submit and request data from their GP practice online. Footfall is currently used by approximately **29 GP Practices in BOB ICB.** It is a reporting tool focused on patient flow and website analytics, integrating with practices and capable of providing over 40 distinct patient form types. In BOB ICB it enables patients to access their GP services without having to visit the practice. Foundation is a "mobile first" product providing key information to patients, and capable of integrating with Footfall to complete patient tasks across multiple devices. Foundation is an enhancement to Footfall providing additional features (compared with the basic Footfall solution) including: • Conforms to NHS Web guidelines. • WCAG 2.1 level AA Compliant • Specialised NHS Blocks • Mobile first design • Integration with NHS Self-help information • Simplified drag and drop editing. • Easier navigation interface By nature, this requires the communication of personal identifiable data, special categories of personal confidential data, including that of minors. Patients will complete online forms to submit information to address their needs without needing an appointment. This could include registering for the practice, requesting prescriptions or submitting health questionnaires. The system will triage patient requests, directing them to the most suitable course of action. Silicon Practice collects GP patient data via a series of contact and submission forms available on the GP Practices web application. The patient selects the form required and inputs their own data. The GP Practice can then respond directly to the patient via the contact details entered by the patient on the form. The GP

	Practice is also able to have a video consultation appointment with the patient. For GP Practices using EMIS, they can use Footfall Connect to reply to a patient and send episodes directly into the patient record.
Are there multiple organisations involved? (If yes – you can use this space to name them, and who their key contact for this work is)**.**	BOB GP Practices Silicon Practice BOB ICB
Can you think of any other Key Stakeholders that should be consulted or involved in this DPIA? (If so then include the details here).	No
Detail anything similar that has been undertaken before?	There are many GP practices that are currently using Footfall for their website and some also include Footfall OC. These systems are used to provide Online "Consultation" to patients as one option for patient access to the GP Surgery. It is an NHS England requirement for GP Practices to provide an OC solution. Click here to enter text.

1. Categories, Legal Basis, Responsibility, Processing, Confidentiality, Purpose, Collection and Use

1.1.

What data/information will be used? Tick all that apply.	Tick or leave blank	**Complete**
Personal Data	✓	1.2
Special Categories of Personal Data	✓	1.2 AND 1.3
Personal Confidential Data	✓	1.2 AND 1.3 AND 1.6
Sensitive Data (usually criminal or law enforcement data)	☐	1.2 but speak to your IG advisor first
Pseudonymised Data	☐	1.2 and consider at what point the data is to be pseudonymised
Anonymised Data	☐	Consider at what point the data is to be anonymised
Commercially Confidential Information	☐	Consider if a DPIA is appropriate
Other	☐	Consider if a DPIA is appropriate

1.2.

Processing has to be lawful so identify which of the following you believe justifies what you are proposing to do and include an explanation as to why in the relevant box. You must select at least one from a – f.

Article 6 (1) of the GDPR includes the following:	
a) THE DATA SUBJECT HAS GIVEN CONSENT	**Tick or leave blank** ☐
Why are you relying on consent from the data subject? Click here to enter text.	
What is the process for obtaining and recording consent from the Data Subject? (How, where, when, by whom). Click here to enter text.	
Describe how your consent form is compliant with the Data Protection requirements? (There is a checklist that can be used to assess this). Click here to enter text.	

b) IT IS NECESSARY FOR THE PERFORMANCE OF A CONTRACT TO WHICH THE DATA SUBJECT IS PARTY (The contract needs to be between the Controller and the individual and not concern data being processed due to someone else having a contract with the Controller. Processing can happen before the contract is entered into e.g. processing a pre-health assessment for a private or cosmetic procedure that is a paid for service with the delivery of that care done under contract between the Patient and the Practitioner).	**Tick or leave blank** ☐
What contract is being referred to? Click here to enter text.	
c) IT IS NECESSARY UNDER A LEGAL OBLIGATION TO WHICH THE CONTROLLER IS SUBJECT (A legal obligation mandates processing of data as a task in itself where there are likely to be legal measures available if not adhered to e.g. an Employer has a legal obligation to disclose salary information to HMRC).	**Tick or leave blank** ☐
Identify the legislation or legal obligation you believe requires you to undertake this processing. Click here to enter text.	
d) IT IS NECESSARY TO PROTECT THE VITAL INTERESTS OF THE DATA SUBJECT OR ANOTHER NATURAL PERSON (This will apply only when you need to process data to protect someone's life. It must be necessary and does not only relate to the individual whose data is being processed. It can also apply to protect another person's life. Emergency Care is likely to fall into this category but planned care would not. You may need to process a Parent's data to protect the life of a child. The individual concerned is unlikely to be able to provide consent physically or legally; if you are able to gain consent then this legal basis will not apply).	**Tick or leave blank** ☐
How will you protect the vital interests of the data subject or another natural person by undertaking this activity? Click here to enter text.	
e) IT IS NECESSARY FOR THE PERFORMANCE OF A TASK CARRIED OUT IN THE PUBLIC INTEREST OR UNDER OFFICIAL AUTHORITY VESTED IN THE CONTROLLER (This is different to 6 c). If you are processing data using this basis for its lawfulness then you should be able to identify a specific task, function or power that is set out in law. The processing must be necessary, if not then this basis does not apply).	**Tick or leave blank** ✓
What statutory power or duty does the Controller derive their official authority from? Health & Social Care Act (Safety and Quality) Act 2015 – Direct Care Provision The legal basis for commissioning purposes: Power to commission certain health services – Power – Section 3A NHS Act 2006: Each ICB has the power to arrange for the provision of such services or facilities as it considers appropriate for the purposes of the health service that relate to securing improvement in – (a) the physical and mental health of persons for whom it has responsibility; or (b) the prevention, diagnosis and treatment of illness in those persons.	
f) IT IS NECESSARY FOR THE LEGITIMATE INTERESTS OF THE CONTROLLER OR THIRD PARTY (Public authorities can only rely on legitimate interests if they are processing for a legitimate reason other than performing their tasks as a public authority. See the guidance for more information about the legitimate interest test).	**Tick or leave blank** ☐
What are the legitimate interests you have? Click here to enter text.	

Article 9 (2) conditions are as follows:	
a) THE DATA SUBJECT HAS GIVEN EXPLICIT CONSENT (Requirements for consent are the same as those detailed above in section 1.2, a))	**Tick or leave blank** ☐
b) FOR THE PURPOSES OF EMPLOYMENT, SOCIAL SECURITY OR SOCIAL PROTECTION (Schedule 1, part 1 of the Data Protection Act 2018 gives more detail on when this can apply to processing and further guidance is available).	**Tick or leave blank** ☐

c) IT IS NECESSARY TO PROTECT THE VITAL INTERESTS OF THE DATA SUBJECT OR ANOTHER NATURAL PERSON WHERE THEY ARE PHYSICALLY OR LEGALLY INCAPABLE OF GIVING CONSENT (Requirements for this are the same as those detailed above in section 1.2, d))	**Tick or leave blank** ☐
d) It is necessary for the operations of a not-for-profit organisation such as political, philosophical, trade union and religious body in relation to its members	*NA*
e) The data has been made public by the data subject	*NA*
f) For legal claims or courts operating in their judicial category	*NA*
g) SUBSTANTIAL PUBLIC INTEREST (Schedule 1, part 2 of the Data Protection Act 2018 gives more detail on when this can apply to processing and further guidance is available).	**Tick or leave blank** ☐
h) PROCESSING IS NECESSARY FOR THE PURPOSES OF PREVENTIVE OR OCCUPATIONAL MEDICINE, FOR THE ASSESSMENT OF THE WORKING CAPACITY OF THE EMPLOYEE, MEDICAL DIAGNOSIS, THE PROVISION OF HEALTH OR SOCIAL CARE OR TREATMENT OR THE MANAGEMENT OF HEALTH OR SOCIAL CARE SYSTEMS AND SERVICES ON THE BASIS OF UNION OR MEMBER STATE LAW OR PURSUANT TO CONTRACT WITH A HEALTH PROFESSIONAL AND SUBJECT TO CONDITIONS AND SAFEGUARDS (Schedule 1, part 1 of the Data Protection Act 2018 gives more detail on when this can apply to processing and further guidance is available).	**Tick or leave blank** ✓
i) PROCESSING IS NECESSARY FOR REASONS OF PUBLIC INTEREST IN THE AREA OF PUBLIC HEALTH, SUCH AS PROTECTING AGAINST SERIOUS CROSS-BORDER THREATS TO HEALTH OR ENSURING HIGH STANDARDS OF QUALITY AND SAFETY OF HEALTH CARE AND OF MEDICINAL PRODUCTS OR MEDICAL DEVICES, ON THE BASIS OF UNION OR MEMBER STATE LAW WHICH PROVIDES FOR SUITABLE AND SPECIFIC MEASURES TO SAFEGUARD THE RIGHTS AND FREEDOMS OF THE DATA SUBJECT, IN PARTICULAR PROFESSIONAL SECRECY (Schedule 1, part 1 of the Data Protection Act 2018 gives more detail on when this can apply to processing and further guidance is available).	**Tick or leave blank** ☐
j) PROCESSING IS NECESSARY FOR ARCHIVING PURPOSES IN THE PUBLIC INTEREST, SCIENTIFIC OR HISTORICAL RESEARCH PURPOSES OR STATISTICAL PURPOSES IN ACCORDANCE WITH ARTICLE 89(1) BASED ON UNION OR MEMBER STATE LAW WHICH SHALL BE PROPORTIONATE TO THE AIM PURSUED, RESPECT THE ESSENCE OF THE RIGHT TO DATA PROTECTION AND PROVIDE FOR SUITABLE AND SPECIFIC MEASURES TO SAFEGUARD THE FUNDAMENTAL RIGHTS AND THE INTERESTS OF THE DATA SUBJECT. (Schedule 1, part 1 of the Data Protection Act 2018 gives more detail on when this can apply to processing and further guidance is available).	**Tick or leave blank** ☐

1.3.

If using special categories of personal data, a condition for processing under Article 9 of the GDPR must be satisfied in addition to a condition under Article 6. You must select at least 1 from a) to c) or g) to i). NOTE: d), e) and f) are not applicable

1.4.

Confirm who the Controller and Processor is/are. Confirm if the Controller/s are solely or jointly responsible for any data processed?

(Identify any other parties who will be included in the agreements and who will have involvement/share responsibility for the data/information involved in this project/activity. Use this space to detail this but you may need to ask your DPO to assist you. Copy and paste the last empty row in the table to add organisations where required (the text has been left unlocked for this purpose on that row only).

Name of Organisation	Role
BOB General Practices	Sole Controller
Silicon Practice	Processor
BOB ICB	Other
Click here to enter text.	Choose an item.

Click here to enter text.	Choose an item.
Click here to enter text.	Choose an item.
Click here to enter text.	Choose an item.

1.5.

Describe exactly what is being processed, why you want to process it and who will do any of the processing?

FootFall and Foundation are platforms for individuals to submit and send data to their GP surgery voluntarily. Anybody can use and submit information on the web applications. Patients are able to submit information about themselves, parents/guardians are able to submit information about their dependents, care homes are able to submit information about their patients, and proxies are able to submit information on behalf of others.

Data below is being processed by Silicon Practice. The purpose of processing is to make admin requirements of a GP Practice more efficient by digitising processes that would require an in-person visit or telephone call. It also increases efficiency for patients by avoiding a physical visit.

Data Type	**Justification**
Name	Patient/Proxy Identification
Date of Birth	Patient/Proxy Identification
Email Address	Communication/Identification
Current and previous address	Patient Identification
Sex	Collected where relevant
Gender	Collected where relevant
Racial/Ethnic Origin	Collected where relevant
NHS Number	Patient Identification
Contact Number	Communication
Relationship to Patient	Proxy Identification
Postcode	Proxy Identification
Information relating to the individuals physical or mental health or condition	Support Patient Care
Photos relating to the individuals physical or condition	Support Patient Care
Information relating to individuals' sexual life	Collected where relevant to the care service requested e.g. sexual health
Information relating to the family life of the individual and the individual's lifestyle and social circumstances	May be provided by patient where relevant to care
Occupational Status	May be provided by patient where relevant to care
Information relating to the individual's religious or other beliefs	May be provided by patient where relevant to care
Information relating to the individual's medication	May be provided by patient where relevant to care

1.6.

Tick here if you owe a duty of confidentiality to any information. ✓

If so, specify what types of information. (e.g. clinical records, occupational health details, payroll information)

Health

Patient information may include demographics like name, date of birth, contact details (email and phone number), and medical history (NHS number, health conditions, medications, etc.), and any other information which may be provided when relevant to care, e.g. family life, occupation status, religious or other beliefs, religious or other beliefs.

1.7.

How are you satisfying the common law duty of confidentiality?

Consent - Explicit

If you have selected an option which asks for further information please enter it here

Patient submits their own data on the form

1.8.

Are you applying any anonymisation/pseudonymisation technique or encryption to any of the data to preserve the confidentiality of any information?

Yes

If you are then describe what you are doing.

Patient data is collected through a series of contact and submission forms. The patient selects the appropriate form and inputs their personal data on to the form they have selected. This could include a combination of personal data and special category personal data or just the former. The form is then stored in either the FootFall or Foundation system and accessible by the GP Practice administrators via an encrypted, authenticated dashboard for processing.

Within the database, the information is all encrypted and is not human-readable and cannot be decrypted without a decryption key. Employee laptops are all password protected and hard drives are encrypted with BitLocker.

All externally stored data is encrypted. A VPN is required to access the dashboard and databases.

Data Retention - The data is encrypted and stored on ISO 27001 certified UK based data centre for 2 years plus the current year before it is destroyed in line with the Records Management Code of Practice for Health and Social Care 2021. Silicon Practice also uses Amazon S3 to store encrypted data backups in a London data centre. These backups are automatically destroyed after 90 days. Video consultations are not recorded and cannot be recorded through FootFall or Foundation, no data from video consultations is retained.

If you don't know then please find this information out as there are potential privacy implications with the processing.

1.9.

Tick here if you are intending to use any information for a purpose that isn't considered as direct patient care. ☐

If so describe that purpose.

Click here to enter text.

1.10.

Approximately how many people will be the subject of the processing?

1000 plus

1.11.

How are you collecting the data? (e.g. verbal, electronic, paper (if you need to add more selections then copy the last 'choose an item' and paste, the text has been left unlocked for you to do this.)

Electronic form

Choose an item.

Choose an item.

Choose an item.

Choose an item.

If you have selected 'other method not listed' describe what that method is.

Click here to enter text.

1.12.

How will you edit the data?

The patient submits their data and it is the data controller's responsibility to ensure the data matches the patient record if editing is required.

1.13.

How will you quality check the data?

Patient submits their data and it is the data controller's responsibility to ensure the data matches the patient record.

1.14.

Review your business continuity or contingency plans to include this activity. Have you identified any risks?

Yes

If yes include in the risk section of this template.

1.15.

What training is planned to support this activity?

Silicon Practice is an existing supplier of Footfall Services to GP Practices and offer customer training. The new Foundation system will be subject to similar capability training to ensure all GP practice users gain the necessary skills to effectively utilise the system. Additionally, Silicon Practice will continue to provide ongoing support to users.

2. Linkage, Data flows, Sharing and Data Opt Out, Sharing Agreements, Reports, NHS Digital

2.1.

Are you proposing to combine any data sets?

No

If yes then provide the details here.

Click here to enter text.

2.2.

What are the Data Flows? (Detail and/or attach a diagram if you have one).

Patient submits form via the GP Practice web application.
The form is stored in either the Footfall or Foundation system
GP Practice administrators access the form via an encrypted, authenticated dashboard for processing.
GP Practice responds directly to the patient via the patient contact details on the form.

FootFall Patient Data Flow (1).pdf

SUMMARY: External Sources (patient) **>** Footfall or Foundation System **>** Internal Operations (Workflow) **>** Patient Records **>** Patient Communication **>** Admin Activity (internal practice management) **>** Archive (As per NHS Records Management Policy)

2.3.

What data/information are you planning to share?

Data Type

Name

- Date of Birth
- Email Address
- Current and previous address
- Sex
- Gender
- Racial/Ethnic Origin
- NHS Number
- Contact Number
- Relationship to Patient
- Postcode
- Information relating to the individuals physical or mental health or condition
- Photos relating to the individuals physical or condition
- Information relating to individuals' sexual life
- Information relating to the family life of the individual and the individual's lifestyle and social circumstances
- Occupational Status
- Information relating to the individual's religious or other beliefs
- Information relating to the individual's medication

2.4.

Is any of the data subject to the National Data Opt Out?

No - it is not subject to the national data opt out

If your organisation has to apply it describe the agreed approach to this

Click here to enter text.

If another organisation has applied it add their details and identify what data it has been applied to

Click here to enter text.

If you do not know if it applies to any of the data involved then you need to speak to your Data Protection Officer to ensure this is assessed.

2.5.

Who are you planning to share the data/information with?

Silicon Practice.

2.6.

Why is this data/information being shared?

The purpose of processing is to make admin requirements of a GP Practice more efficient by digitising processes that would require an in-person visit or telephone call. It also increases efficiency for patients by avoiding a physical visit.

2.7.

How will you share it? (Consider and detail all means of sharing)

Via web GP Practice web application form

Tick if you are planning to use Microsoft Teams or another similar online networking/meeting solution that may have the facility to store or record conversations or related data as part of the sharing arrangements ☐

Provide details of how you have considered any privacy risks of using one of these solutions

The Privacy risks have been considered. The primary data sharing is with the patient's own GP practice to allow the GP to deliver online consultations or video consultations. Silicon Practice emphasises that they do not share any personal identifiable information with anyone beyond what is necessary to deliver their services or comply with legal obligations. Any information sharing for the purposes of collecting statistics on the performance of their platform, or counting user traffic, e.g. to NHS Digital, is anonymised.

Silicon Practice have detailed Privacy notice on their website emphasising data security **https://www.siliconpractice.co.uk/privacy-notice/** and their Data Processing Agreement **Data Processing Agreement - Silicon Practice | Digital Solutions for GP Practices** details how they comply with data protection requirements when delivering their services to Practices.

2.8.
What data sharing agreements are or will be in place?
Not applicable – Direct Care

2.9.
What reports will be generated from this data/information?
None

2.10.
Are you proposing to use Data that may have come from NHS Digital (e.g. SUS data, HES data etc.)?
No

If yes, are all the right agreements in place?
Choose an item.

Give details of the agreement that you believe covers the use of the NHSD data
Click here to enter text.

If no or don't know then you need to speak to your Data Protection Officer to ensure they are put in place if needed.

3. Data Processor, IG Assurances, Storage, Access, Cloud, Security, Non-UK processing, DPA

3.1
Are you proposing to use a third party, a data processor or a commercial system supplier?
Yes

If yes use these spaces to add their details including their official name and address. If there is more than one then include all organisations. If you don't know then stop and try and find this information before proceeding.
Schappit Ltd (Silicon Practice Digital Health Solutions)

Schappit Ltd
Unit 2, 79-93 Ratcliffe Road
Sileby
Loughborough
Leicestershire LE12 7PU

3.2
Is each organisation involved registered with the Information Commissioner? Copy and paste the last empty row in the table to add organisations where required (the text has been left unlocked for this purpose on that row only)

Name of organisation	Registered	Registration details or comments if not registered
Schappit Ltd (Silicon Practice Digital Health Solutions)	Yes	ZA074234
Click here to enter text.		Click here to enter text.

Click here to enter text.	Choose an item.	Click here to enter text.
Click here to enter text.	Choose an item.	Click here to enter text.
Click here to enter text.	Choose an item.	Click here to enter text.
Click here to enter text.	Choose an item.	Click here to enter text.

3.3

What IG assurances have been provided to you and does any contract contain IG clauses that protect you as the Controller? (e.g. in terms and conditions, their contract, their tender submission). Copy and paste the last empty row in the table to add organisations where required (the text has been left unlocked for this purpose on that row only)

Name of organisation	Brief description of assurances obtained
Schappit Ltd (Silicon Practice Digital Health Solutions)	DTAC, contract, DSPT completion. Silicon Practice has a number of internal policies that address confidentiality, integrity, availability and resilience of processing systems and services. Silicon Practice is compliant with the Data Security & Protection Toolkit to ensure NHS data processing standards are met. Silicon Practice has also achieved and maintains ISO27001 and Cyber Essentials plus as specified by the NHS and all Silicon Practice employees complete as a minimum, annual Information Security and Data Protection training/awareness courses.
Click here to enter text.	Click here to enter text.
Click here to enter text.	Click here to enter text.
Click here to enter text.	Click here to enter text.
Click here to enter text.	Click here to enter text.
Click here to enter text.	Click here to enter text.

3.4

What is the status of each organisation's Data Security Protection Toolkit?

DSP Toolkit

Copy and paste the last empty row in the table to add organisations where required (the text has been left unlocked for this purpose on that row only)

Name of organisation	ODS Code	Status	Published date
Schappit Ltd (Silicon Practice Digital Health Solutions)	8KC12	Standards Met	31/03/2023
Click here to enter text.	Click here to enter text.	Click here to enter text.	Click here to enter text.
Click here to enter text.	Click here to enter text.	Click here to enter text.	Click here to enter text.
Click here to enter text.	Click here to enter text.	Click here to enter text.	Click here to enter text.
Click here to enter text.	Click here to enter text.	Click here to enter text.	Click here to enter text.
Click here to enter text.	Click here to enter text.	Click here to enter text.	Click here to enter text.

3.5

How and where will the data/information be stored? (Consider your answer to 2.7 and the potential storage of data in any online meeting or networking solution).

The data is encrypted and stored on ISO 27001 certified UK based data centre. Silicon Practice also uses Amazon S3 to store encrypted data backups in a London data centre. These backups are automatically destroyed after 90 days. Video consultations are not recorded and cannot be recorded through FootFall or Foundation, no data from video consultations is retained. All video consultation communication is conducted over HTTPS using TLS and because we are using relayed sessions the connection is P2P (Peer to Peer) and

there is no middleman managing the connection. Silicon Practice are not storing any video data so a higher level of encryption over and above HTTPS is not required.

3.6
How is the data/information accessed and how will this be controlled?

Silicon Practice DevOps staff have full access to the backups and servers and the encrypted data contained therein, and the development team has limited access to the servers and the encrypted data contained therein. Access is restricted to authorised staff only for the purpose of maintaining and supporting the web application and for data processing at the documented instructions of the data controller only.

3.7
Is there any use of Cloud technology?
Yes

If yes add the details here.
Amazon S3. Silicon Practice has data processing agreements with their sub-processors and ensure compliance with Data Protection Legislation which is included in the agreement.

3.8
What security measures will be in place to protect the data/information?

The data is encrypted and stored on ISO 27001 certified UK based data centre. Silicon Practice also uses Amazon S3 to store encrypted data backups in a London data centre. These backups are automatically destroyed after 90 days. Video consultations are not recorded and cannot be recorded through FootFall or Foundation, no data from video consultations is retained. All video consultation communication is conducted over HTTPS using TLS and because we are using relayed sessions the connection is P2P (Peer to Peer) and there is no middleman managing the connection. Silicon Practice are not storing any video data so a higher level of encryption over and above HTTPS is not required.

Silicon Practise are also DSP Toolkit compliant, maintains ISO27001 and Cyber Essential Plus accreditation, Retains Data Processing Agreements with all sub-processors and ensure all staff complete as a minimum annual Information Security and Data Protection training/awareness courses. Additionally Silicon Practice has undertaken a DTAC assessment as part of this DPIA process.

Is a specific System Level Security Policy needed?
No

If yes or don't know then you need to speak to your Data Protection Officer to ensure one is put in place if needed.

3.9
Is any data transferring outside of the UK? (you must determine this so only select don't know if you have further investigations to make but the DPIA will not be approved without this information)
No

If yes describe where and what additional measures are or will be in place to protect the data.
Click here to enter text.

3.10
What Data Processing Agreement is already in place or if none, what agreement will be in place with the organisation and who will be responsible for managing it?

Silicon Practice's Data Processing Agreement is published on their website. Any variation from this Agreement would be captured on the Call Off Order Form dated 22 April 2022.

4. Privacy Notice, Individual Rights, Records Management, Direct Marketing

4.1

Describe any changes you plan or need to make to your Privacy Notice and your proposed completion date? (There is a checklist that can be used to assess the potential changes required or if you wish for it to be reviewed then add the link below).

The ICB do not need to make any changes to their Privacy Notice.

Silicon Practice has a Privacy Notice in place **www.siliconpractice.co.uk/privacy-notice/** .

The Data Controllers may need to take advice from their DPO relating to updating their Privacy Notices.

4.2

How will this activity impact on individual rights under the GDPR? (Consider the right of access, erasure, portability, restriction, profiling, automated decision making).

No impact. Individual Rights remain the responsibility of the Data Controllers

4.3

How long is the data/information to be retained?

Silicon Practice retain the encrypted data for 2 years plus current year. Video consultations are not recorded therefore no data is retained.

4.4

How will the data/information be archived?

Not applicable

4.5

What is the process for the destruction of records?

Silicon Practices securely destroy records in line with the Records Management Code of Practice for Health and Social Care 2021.

4.6

What will happen to the data/information if any part of your activity ends?

Silicon Practice retain personal information only for as long as necessary to fulfil the purpose it was collected for. Backed up data is encrypted and retained for 90 days and stored in a secure UK data centre before being automatically destroyed. Video consultations are not recorded and cannot be recorded through Footfall or Foundation, so there is no data from video consultations to be retained.

4.7

Will you use any data for direct marketing purposes? (you must determine this so only select don't know if you have further investigations to make but the DPIA will not be approved without this information)

No

If yes please detail.

Click here to enter text.

5. Risks and Issues

5.1

What risks and issues have you identified? The DPO can provide advice to help complete this section and consider any measures to mitigate potential risks.

The risks 1 – 17 below have been provided by Silicon Practice and are included in their DPIA. Additional risk identified by the ICB.

Describe the source of risk and nature of potential impact on individuals. (Include associated compliance and corporate risks as necessary and copy and paste the complete bottom row to add more risks (the text has been left unlocked in both tables to enable you to do this)).	**Likelihood of harm**	**Severity of harm**	**Overall risk**
1.A patient-submitted form is accidentally sent to an incorrect email address	Possible	Significant	Medium
2.A patient form is downloaded as a PDF and kept in an insecure format e.g. USB, printed, saved on local PC.	Possible	Significant	Medium
3.Intruder break into Silicon Practice office/home and finds system login information.	Remote	Severe	Medium

4.A visitor to an employee's place of work catches a glimpse of patient data on screen.	Remote	Minimal	Low
5.Footfall or Foundation login information to a dashboard is sent to the wrong recipient	Remote	Significant	Low
6.The Silicon Practice system is hacked.	Possible	Severe	High
7.A Silicon Practice employee takes notepad from home/office that contains login information to a sensitive system and loses the notepad in a public place.	Possible	Significant	Medium
8.There is a security breach affecting all Wordpress sites	Probable	Severe	High
9.A disgruntled Silicon Practice employee leaks login information to Silicon Practice systems.	Remote	Severe	Medium
10.Data stored on an external server is breached.	Possible	Severe	High
11.A Silicon Practice laptop is left logged in and unattended in a public place.	Remote	Minimal	Low
12.A Silicon Practice employee sees live PII data on a customer's site or database that is not relevant to the task at hand.	Possible	Minimal	Medium
13.A systems admin could overwrite the wrong database during a data restore procedure.	Possible	Severe	High
14.A Silicon Practice employee installs malicious software that mines data on the company network.	Possible	Severe	High
15.Unauthorised people/contractors accessing patient information from Silicon Practice employees' laptops.	Possible	Severe	High
16.Theft in employee's home of a Silicon Practice laptop.	Possible	Significant	Medium
17.Staff that are authorised to access data may use their access to access data they are not supposed to.	Remote	Significant	Medium
Disruption of patient care – patients scheduled for consultations may not be able to connect with their Practice, leading to delays in diagnosis, treatment or repeat medication which would be critical for urgent or chronic conditions.	Possible	Significant	Medium
Patients may become frustrated and anxious if their consultation is interrupted or rescheduled due to a system outage. This can negatively impact patient satisfaction and trust.	Possible	Significant	Medium
Loss of Patients consultations (eg requests for prescription, referrals, request for appointments, results, etc) as a result of the system going down?	Possible	Significant	Low

5.2

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in 5.1

The Silicon Practice risk 1 -17 mitigations below have all had the measures agreed by Silicon Practice. Additional risks mitigated by the ICB.

Risk	Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure approved (SIRO)
1.A patient-submitted form is accidentally sent to an incorrect email address.	The surgery is able to respond to a patient form, and in order for the patient to view the response, the patient's date of birth must be entered. If the owner of the incorrect emails address does not know the patient, they are unable to view the message as they will not know the date of birth. There are only 3 attempts at entering the correct date of birth before the system locks the user out. After an agreed period of time that is set by each individual Practice, the link will expire	Reduced	Low	Choose an item.
2.A patient form is downloaded as a PDF and kept in an insecure format e.g. USB, printed, saved on local PC.	Employees with access to the dashboard are given training on how to safely handle files and devices that could contain patient data to prevent this happening. Furthermore, the data in a downloaded PDF will only contain the contents of the form that was submitted and nothing else, limiting the kind of information available. Patient data is anonymised to further mitigate risk. All stand users have USB controls in place so they cannot write to USB devices. This can only be over-ridden by administrators.	Reduced	Low	Choose an item.
3.An intruder breaks into the Silicon Practice office/home and finds system login information.	Dashboard access is restricted to the NHS network, Practice IP address and specific addresses that have been whitelisted by DevOps. Therefore it cannot be accessed publicly.	Reduced	Low	Choose an item.
4.A visitor to an employee's place of work catches a glimpse of patient data on a screen.	Visitors are only brought into the working space when it is absolutely necessary. We have separate office area where visitors are taken and meetings are held, there are no PCs or files in this area. Most work on Silicon Practice sites are done in preview environments where patients will not have submitted any information. Any work done to a live site very rarely, if ever, requires viewing patient information and staff are trained to understand the importance of keeping this information confidential.	Tolerated	Low	Choose an item.

5.Footfall and Foundation Login information to a dashboard is sent to the wrong recipient.	Dashboard access is restricted to the NHS network and Practice IP addresses, so it cannot be accessed publicly.	Tolerated	Low	Choose an item.
6.The Silicon Practice system is hacked.	Penetration tests are undertaken to test the security of the product and the platform. Penetration tests are performed annually or on significant change. Other security features such as brute force detection and limited external attach surface. All data is also encrypted. Other security features are listed in the mitigations for risks 3, 10, 13, 14 and 17.	Reduced	Medium	Choose an item.
7.A Silicon Practice employee takes a notepad from the office/home that contains login information to a sensitive system and loses the notepad in a public place.	Silicon Practice use LastPass as a secure and encrypted way to share login details. LastPass requires a personal login and 2-factor authentication before being able to access the login information for any other Silicon Practice systems. Passwords are handled digitally, there is no need to write down login details on a piece of paper. Dashboard access is restricted to NHS network, Silicon Practice VPN and Practice IP addresses, so it cannot be accessed publicly.	Reduced	Low	Choose an item.
8.There is a security breach affecting all Wordpress sites.	The Footfall and Foundation front ends are built in WordPress, which is open source and regularly updated with security fixes. Silicon Practice always tests the latest version of WordPress that they wish to use in a test environment before pushing it to live web applications. We get alerted to all serious WordPress and plugin bugs through InfiniteWP and patch accordingly. We currently follow a process to update WordPress sites periodically.	Reduced	Low	Choose an item.
9.A disgruntled Silicon Practice employee leaks login information to Silicon Practice systems.	In the Silicon Practice Employee Handbook there is an official grievance procedure so that any issues relating to unhappiness, unfairness, dissatisfaction, and so on, can be dealt with through the proper channels. There is also an official policy on information confidentiality that details how an employee is expected to act with this sort of data. Dashboard access is restricted to the NHS network, Silicon Practice VPN and Practice IP addresses, so it cannot be accessed publicly.	Tolerated	Low	Choose an item.
10.Data stored on an external server is breached.	All externally stored data is encrypted. A VPN is required to access the dashboard and databases.	Reduced	Low	Choose an item.

11.A Silicon Practice laptop is left logged in and unattended in a public place.	Silicon Practice employees are trained not to leave work devices unattended and to lock the device when not in use. Laptops also self-lock after a set period. Dashboard access is restricted to the NHS network and Practice IP addresses, so it cannot be accessed publicly.	Tolerated	Low	Choose an item.
12.A Silicon Practice employee sees live PII data on a customer's site or database that is not relevant to the task in hand.	Silicon Practice employees do not view data that is not relevant to the task in hand. On newer site dashboards, there is a procedure whereby information of worklist items is not visible to Silicon employees unless they search for a specific episode IDs, patient surnames, etc to find the relevant episodes. This is currently being improved upon and further solutions will eventually apply to all sites that have the necessary code applied. Within the database, the information is all encrypted and so is not hum-readable. Thus it cannot be read nor decrypted without a decryption key.	Reduced	Low	Choose an item.
13.A systems admin could overwrite the wrong database during a data restore procedure.	System administrators will use accounts that only have permissions to work on the database that is required. As each site uses a unique encryption key no patient data would be displayed to the wrong Practice	Reduced	Low	Choose an item.
14.A Silicon Practice employee installs malicious software that mines data on the company network.	Silicon Practice use Sophos endpoint protection that protects the workstations against malware and ransomware. USB devices are also disabled by default.	Reduced	Low	Choose an item.
15.Unauthorised people/contractors accessing patient information from a Silicon Practice employee's laptop.	Unauthorised people in an employee's house should not be able to see patient information. When away from their laptops employees must always lock their screen. At all times, staff must avoid letting other people view their screens. There are very few situations that would require staff members to view patient data. Staff are trained to understand the importance of keeping this information confidential. Staff are also trained that notes on paper must not contain any sensitive data and if they contain any company confidential data they are to be locked in a safe drawer or destroyed, not left lying around.	Reduced	Low	Choose an item.
16.Theft in employee's home of a Silicon Practice laptop.	Theft of a Silicon Practice laptop from employee homes is possible. Laptops are all password protected and hard drives are encrypted with BitLocker.	Reduced	Low	Choose an item.

17.Staff that are authorised to access data may use their access to access data they are not supposed to.	Silicon Practice DevOps team monitor access that staff have to information. Logs are kept of the DevOps database access to track who has accessed the data.	Reduced	Low	Choose an item.
BUSINESS CONTINUITY RISKS AND MITIGATIONS – REVIEWED UNDER SECTION 1.14				
Disruption of patient care – patients scheduled for consultations may not be able to connect with their Practice, leading to delays in diagnosis, treatment or repeat medication which would be critical for urgent or chronic conditions.	Having a backup system in place allows for a quick switch to an alternative platform in case of a primary system outage. Practices would be able to connect with the patient via telephone, MS Teams, a home visit to the patient or ask patient to visit the Practice. Clinicians scheduled to see patients could also request forms be resubmitted.	Reduced	Low	Choose an item.
Patients may become frustrated and anxious if their consultation is interrupted or rescheduled due to a system outage. This can negatively impact patient satisfaction and trust.	To lower the risk of patient anxiety and frustration, the practice could send automated notifications or text messages, switch to phone consultations or issue temporary refills for prescriptions.	Reduced	Low	Choose an item.

5.3

What if anything would affect this piece of work?

Nothing identified. The FootFall platform is widely used in the NHS and its core functionality remains the same. This DPIA focuses on the upcoming upgrade, the Foundation System. This enhancement aims to improve the patient experience by streamlining information input. It is important to note the underlying system and its operations will not be affected by this upgrade.

5.4

Please include any additional comments that do not fit elsewhere in the DPIA?

Silicon Practice uses the following Sub-Processors. Data Protection and Security assurance is included in the Data Processing Agreement **https://www.siliconpractice.co.uk/data-processing-agreement/**

Amazon – web housing and storage
4D – web housing and storage
Atlassian – Service Desk, Ticketing and Task Management
Google Suite – Email, Documents and File Storage
Wirehive – Web Hosting and Storage
Redcentric – HSCN Connection
Docman – Data Handler
Brinkworth Virtual Business Centre – Disaster Recovery/Out of Hours Telephony
OpenTok – Video Consultation

BT Soprano – SMS Messaging
CarelS – Clinical Systems Integration
Amazon SES – Email Messaging
Zoho Corporation – CRM Systems, Finance, Email, Statistics.

6. Consultation

6.1
Have you consulted with any external organisation about this DPIA?
No

If yes, who and what was the outcome? If no, detail why consultation was not felt necessary.
Click here to enter text.

6.2
Will you need to discuss the DPIA or the processing with the Information Commissioners Office? (You may need the help of your DPO with this)
No

If yes, explain why you have come to this conclusion.
Click here to enter text.

7. Data Protection Officer Comments and Observations

7.1 Comments/observations/specific issues	[redacted], GP DPO – dated 02 May 2024] review of the DPIA – Noted one medium risk 5.2 (6) reduced from high. DPO recommendation is to ensure that this risk is reduced, in future, to low. Noted the valid reason provided from a security standpoint. I've noted it is not subject to the national data opt out. GP practices **must update** their Privacy Notice to inform their patients. Suggested text: Purpose : Silicon Practice provides an Online Consultation (OC) solution that is integrated to the Footfall Practice website for GP Surgeries. They allow patients to submit and request data from their GP practice online. Patients will complete online forms to submit information to address their needs without needing an appointment. This could include registering for the practice, requesting prescriptions or submitting health questionnaires. The system will triage patient requests, directing them to the most suitable course of action. Silicon Practice collects GP patient data via a series of contact and submission forms available on the GP Practices web application. The patient selects the form required and inputs their own data. The GP Practice can then respond directly to the patient via the contact details entered by the patient on the form. It is also used as a reporting tool focused on patient flow and website analytics, integrating with practices and capable of providing over 40 distinct patient form types. In BOB ICB it enables patients to access their GP services without having to visit the practice.

	Lawful basis for processing data This DPIA has confirmed the following: Article 6 (1) (e) Legitimate interests It is necessary for the performance of a task carried out in the public interest or under official authority vested in the controller Article 9 (2) (h) Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of union or member state law or pursuant to contract with a health professional and subject to conditions and safeguards. [redacted], BOB ICB DPO]: The comments and observations by the GP DOP are noted and supported.

8. Review and Outcome

Based on the information contained in this DPIA along with any supporting documents, you have determined that the outcome is as follows:
A) There are no further actions needed and we can proceed

If you have selected item B), C) or D) then please add comments as to why you made that selection
Click here to enter text.

We believe there are
Choose an item.

If you have selected item B) or C) then list these in the amber boxes below and then consider additional measures you could take and include these in the green boxes below

Residual risks and nature of potential impact on individuals. (Include associated compliance and corporate risks as necessary and copy and paste the complete bottom row to add more risks (the text has been left unlocked in both tables to enable you to do this)).	**Likelihood of harm**	**Severity of harm**	**Overall risk**
Click here to enter text.	Choose an item.	Choose an item.	Choose an item.
Click here to enter text.	Choose an item.	Choose an item.	Choose an item.
Click here to enter text.	Choose an item.	Choose an item.	Choose an item.
Click here to enter text.	Choose an item.	Choose an item.	Choose an item.

Additional measures you could take to reduce or eliminate residual risks identified as medium or high risk above (B and C)				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved (SIRO)**
Click here to enter text.	Click here to enter text.	Choose an item.	Choose an item.	Choose an item.
Click here to enter text.	Click here to enter text.	Choose an item.	Choose an item.	Choose an item.

Click here to enter text.	Click here to enter text.	Choose an item.	Choose an item.	Choose an item.
Click here to enter text.	Click here to enter text.	Choose an item.	Choose an item.	Choose an item.

Signed and approved on behalf of Oxfordshire Buckinghamshire and Berkshire West Integrated Care Board

Name: [redacted]

Job Title: Data Protection Officer

Signature: Date: 02/05/2024

Signed and approved on behalf of [redacted]

Name: Click here to enter text.

Job Title: Click here to enter text.

Signature: Click here to enter text. Date: Click here to enter a date.

Please note:

You should ensure that your Information Asset Register and Data Flow Mapping Schedules are updated where this is relevant.

This DPIA can be disclosed if requested under the Freedom of Information Act (2000). If there are any exemptions that should be considered to prevent disclosure detail them here:
Click here to enter text.