## **Data Privacy Impact Assessment (DPIA)**

CLOUD BASED TELEPHONE SYSTEM WITH CLINICAL INTEGRATION AND AUTOMATED APPOINTMENT BOOKING AND PRESCRIPTION ORDERING

# Submitting controller details

|  |  |
| --- | --- |
| Name of controller | The Scott Practice |
| Subject/title of DPIA | **Cloud based telephony and clinical system integration** |
| Name of controller contact /DPO  (delete as appropriate) | The Scott Practice  The Practice Data Protection Officer is Caroline Million. Any queries regarding Data Protection issues should be addressed to her at: -  Email: [caroline.million@nhs.net](mailto:caroline.million@nhs.net) |

# Step 1: Identify the need for a DPIA

|  |
| --- |
| Explain broadly what 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. Summarise why you identified the need for a DPIA. |
| * Patient Partner is a software application that can communicate with a medical practice information system (MPIS) and a telephone system. It includes two modules that process personal data (1) appointments and (2) repeat prescriptions. * It provides an automated system that enables patients registered at a practice to book, check, change and cancel appointments, and order repeat prescriptions, using a touch tone telephone. * PP uses dedicated phone lines and does not require any staff intervention, therefore Patients will be able to book appointments 24 hours a day, 7 days a week and the service will reduce the workload of reception staff and improve access to patients. * The system is similar to online appointment booking – it is just using a telephone rather than an app or website * When telephoning the practice the patients will be offered a choice to select Option 1 if they wish to use the automated booking system (patients will still have the option to hold to speak to a receptionist) * Patients will confirm their identity by entering their date of birth. * The system (Patient Partner) will integrate with the clinical system (Emis) to confirm the patient identity and to access available appointments * Patients will be offered a choice of selections as to which clinician they wish to see and will be offered a choice of available appointments which they can accept or decline. Once accepted the patient will be booked into that slot on the clinical system (Emis) * The telephone system will integrate with Emis to provide a telephone number recognition so when the patient rings the system will recognise the number and automatically open the patient record in Emis. This will reduce errors and speed up the manual process of selecting a patient. * The legal basis for this is Article 6 1 9 € and article 9 2 (h) of UK GDPR |

# 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 other way of describing data flows. What types of processing identified as likely high risk are involved? |
| A patient calls the practice and selects PP.  PP requests the patient to key in their date-of-birth and (normal contact) telephone number. (A patient can call the medical practice and use PP from any telephone.)  PP uses this information to interrogate the MPIS, to identify a patient with matching details.  PP then presents a telephone menu to the caller, to enable the caller to book, check, change or cancel an appointment and/or to order repeat prescriptions.  PP interrogates the MPIS to do one or both of the following. (1) Determine available appointment times. The caller selects an appointment time and PP records this in the MPIS. (2) Determine repeat prescription medical treatments, from which the patient may re-order. The caller selects one or more repeat treatments and PP records this in the MPIS. |

|  |
| --- |
| **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? |
| * The scope of the service relates to any registered patient who opts to use the service * PP records information resulting from all calls into a database for reporting. PP records the following person identifiable information, and other information, into the database * . Patient ID NHS Number Date of Birth Partial Telephone Number   Details of Appointments Details of Repeat Prescriptions   * (1) The Reporting Database consists of information that is also recorded in the MPIS. * (2) Access to the Reporting Database is restricted. ( * 3) The Reporting Database is NOT transferred outside the medical practice. Reports that consist of summary and statistical information, derived from the Reporting Database, but which do NOT contain any personal information, are sent from the medical practice to Voice Connect for maintenance and reporting purpose   PP also records log files. These are stored in an encrypted form on the local machine. Log files record the telephone number of each call but no other person identifiable information. They are usually kept 7–30 days before automatic deletion. (They are required for investigation if a patient reports an error). |
|  |

|  |
| --- |
| **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)? |
| * The data relates to patients of the practice who choose to use the system. It is envisaged that for children the majority of contact would be made by the parent/guardian on the child’s behalf. * This service is not novel, patient partner is already installed in many practices. * No clinical information is extracted from the patient record * No data leaves the UK   The benefits provided by PP augment the existing service. PP does not create or destroy data: the database it compiles for reporting is a record of activity that duplicated information recorded in the MPIS. |
|  |

|  |
| --- |
| **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? |
| * To increase access to the practice by offering patients an alternative way to book appointments * Patients will have access to book appointments 24 hours a day/7 days a week * To improve access to patients * To reduce reception workload |

# 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? |
| The practice will be advertising PP on our website, social media and in the surgery to promote the uptake of the service but patients will still be able to choose not to use the system. |

# 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? |
| * Article 5 – Item 1 – Principles * (a) Compliant (b) Compliant (c) Compliant (d) Compliant NOTE PP has little control over integrity of data. It does not hold its own data; PP accesses data held by the MPIS. (e) Compliant (f) Compliant * Article 6 – Item 1 – Lawfulness of Processing * (1) The lawful basis for processing is: * (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. (2) There are two alternatives to the use of PP, but they differ substantially: (a) Practice staff can take calls, but only during daytime working hours and if they are able to answer an incoming call; (b) Web interface and smart device apps provided by the producers of MPISs, which require internet access or a data connection. * Minimisation of Data * PP only transiently accesses the minimum required personal data during a call. * Function Creep * The functionality of PP is inherently limited. |

# Step 5: Identify and assess risks to rights and freedoms of data subjects (patients)

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Transparent information, communication and modalities for the exercise of the rights of the data subject  Information to be provided where personal data are collected from the data subject  Information to be provided where personal data have not been obtained from the data subject  Right of access by the data subject  Right to rectification  Right to erasure (‘right to be forgotten’)  Right to restriction of processing  Notification obligation regarding rectification or erasure of personal data or restriction of processing  Right to data portability  Right to object  Automated individual decision-making, including profiling  Restrictions | PP uses data recorded in the MPIS and has little or no effect upon existing arrangements to provide to a patient, communications and exercise of rights, with respect to that data.  PP uses data recorded in the MPIS to enable patients to call the automated system to manage appointments and (if available) to order repeat prescriptions. It performs automated processing but not automated decision making. PP confirms arranged appointments and ordered repeat prescriptions during a call.  Information added to the MPIS that is not obtained from a patient, is information that is added by the medical practice, which should be communicated to the patient, either during a consultation or by some other method. PP has no effect on this  PP can confirm existing appointments. PP uses data recorded in the MPIS, and does not affect an existing arrangement, to provide to a patient, access to that data  PP enables a patient to change and cancel existing appointments. PP uses data recorded in the MPIS and does not affect an existing arrangement, to provide to a patient, rectification of that data  NOT APPLICABLE TO DATA HELD BY AN NHS BODY. Processing of personal data by an NHS body is necessary according to GDPR, Article 17, Paragraph 3, Items (c) and (d). Therefore, Paragraph 1 does not apply. Paragraph 2 is not relevant. Therefore, a person does not have the right to request an NHS body to erase any personal data (from their medical records).  PP uses data recorded in the MPIS and does not affect an existing arrangement, to provide to a patient, the right to restriction of processing of that data.  PP uses data recorded in the MPIS and does not affect an existing arrangement, to provide to a patient, notification regarding rectification or erasure of that data.  PP uses data recorded in the MPIS and does not affect an existing arrangement, to provide the right to a patient, to portability of that data.  PP uses data recorded in the MPIS and does not affect an existing arrangement, to provide the right to a patient, to object to processing of that data  PP uses data recorded in the MPIS and does not affect an existing arrangement to provide the right to a patient, to not to be subject to a decision based solely on automated processing, including profiling, of that data.  PP uses data recorded in the MPIS and does not affect an existing arrangement to provide any restriction of that data. |  | | Low  Low  None  None  None  Not applicable  None  None  None  None  None  none | | Accept  Accept  Accept  Accept  Accept  N/A  Accept  Accept  Accept  Accept  Accept  accept | |
|  | | |  |  |  | |

# Step 7: Sign off and record outcomes

|  |  |
| --- | --- |
| DPO advice:  MILLION, Caroline (LOCALA COMMUNITY PARTNERSHIPS CIC)  Thu 4/14/2022 13:51    To:   * FELLS, Rose (THE SCOTT PRACTICE)   Hi Rose    I am happy with the product, I have looked at the website and read their privacy notice.    Regards  Caroline    Caroline Million    Independent DPO and IG Specialist  [Caroline.million@outlook.com](mailto:Caroline.million@outlook.com)  07912 975522    **From:** FELLS, Rose (THE SCOTT PRACTICE) <rose.fells@nhs.net> **Sent:** 14 April 2022 10:03 **To:** MILLION, Caroline (LOCALA COMMUNITY PARTNERSHIPS CIC) <caroline.million@nhs.net> **Subject:** DPIA for sign off    Hi  Please find attached DPIA for our new telephone system which includes a telephone based automated appointment booking and repeat prescription ordering solution  DPO Signature: Caroline Million | |
| DPO advice accepted or overruled, if overruled provide reasons: |  |
|  | |
| This processing and this DPIA will be kept under review, next review date: |  |