PIA - Bridlington PCN

Section 1 - Page Properties:

PIA Created	28/06/2019
Department / Squad	Operations/Legal
Creator / Owner	Director of Risk and Governance, Push Doctor

Section 2 - Screening Questions:

Complete Sections 2A and 2B in full to identify whether a full PIA needs to be completed.

	Section 2A	
1	**Summarise what the activity aims to achieve? (What is the benefit to Push Doctor, our users and/or other parties?)** **- Use this to help to define why there is a legitimate interest undertaking this new or amended processing of personal data.**	Partnership between Push Doctor and Bridlington PCN to provide remote GP /digital consultations to Bridlington PCN patients, through the use of the Push Doctor application
2	**Attach Confluence Link (and/or other Links to information about the activity).**	NA

3	**Summarise why the need for a PIA was identified.**	Processing of sensitive personal data Data Sharing

	Section 2B	**Answer Yes or No only - details can be collected later if necessary**
1	**Will the activity involve the collection of new information about individuals?** **Note: Re-use of data collected for one purpose but now being used for another is covered by Q4.**	Yes
2	**Will the activity compel individuals to provide information about themselves?**	Yes
3	**Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?** **This could also cover situations where an organisation is providing Push Doctor with information they haven't supplied to a third party before.**	Yes
4	**Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?**	No
5	**Does the activity involve you using new technology or technology that might be perceived as being intrusive?** **- Intrusion can cover genetics, biometrics and the tracking or monitoring of behaviour or communications (whether by post, phone or online and extends to monitoring the records of senders and recipients as well as the content of messages). It can also include the collection of information through the surveillance or monitoring of how people act in public or private spaces.**	Yes

6	**Will the activity result in you making decisions or taking action against individuals in ways which can have a significant impact on them?** **- If you are unsure what would count as a significant impact please consult with the DPO.**	Yes
7	**Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations?** **For example will any of the information processed be data that people would consider private, or that would fall under the definition of sensitive data (racial or ethnic origin; political opinions; religious or philosophical beliefs; trade-union membership; genetic data; biometric data (Where used for ID purposes); health; sex life; or sexual orientation)?**	Yes
8	**Will the project require you to contact individuals in ways which they may find intrusive?** **- For example profiling, cold calling and marketing by email or SMS.**	No

Section 3 - Impact Assessment:

	Section 3 **Complete this section only if you have answered Yes to a question in Section 2B**	
1	**List the types of data subjects whose data will be processed** **(eg. Employees, Current Customers, Prospective customers etc.)**	NHS patients of Bridlington PCN Employees

2	**Identify / describe each item of personal data to be processed.** **(eg. Employee Name, Address, Current Customer Payment History, Prospective Customer Medical Information etc.)**	Registration: Patient name Patient Address Patient Mobile number Date of birth Email Consultation: Details of illness or ailments provided during consultation with PD G.Ps Feedback: Patient comments regarding the service and their experience Data Sharing – PD to Practice: Patient's name Patient's date of birth Patient's mobile phone number Patient's email address GP Name GP GMC registration number
3	**What is the source of personal data (at point of collection or receipt)?** **(Where are we getting the information from?)**	Patients will register directly on the PD portal after being notified by the practice of the operational service being available Consultation: Directly from patient during a consultation

4	**What is the approximate volume of data subjects whose data will be processed?** **- Include day/week/month as appropriate.**	53 appointments per week across Bridlington PCN 6 surgeries
5	**Is this personal or sensitive data?** **- Select only from list** **(Sensitive data = Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.)**	Personal data Sensitive personal data Confidential data

6	**What is Push Doctor's role in this circumstance?** **- Select only from list** **Data Controller: The entity (in most cases, an organisation) that directs the reason why personal data is processed in the first place.** **Data Processor: The entity (in most cases an organisation) that processes data on behalf of a data controller (e.g confidential waste removal, or cloud storage provider)** **Joint Data Controllers: Where two or more data controllers jointly determine the purposes and means of processing, they are joint controllers (e.g Push Doctor and the Modality partnership)** **For additional support, Contact Director of Risk and Governance.**	Data Processor when processing on Practice clinical systems Data Controller

7	**Processing activity (What are we going to do with the data?)** **- Select only from list** **For additional support, Contact Director of Risk and Governance.**	Registration: Collection/transmission Consultation: Collection/transmission
8	**What is the purpose of this processing?** **- Refer to your answer to Section 2A Q1 and summarise purpose.**	Bridlington PCN practices will send a 'now available' text to all mobile numbers stored in their clinical system. Upon receiving the text, patients can then register directly with PD Consultation: During consultation, the PD GP has access to write directly to the clinical system. The sensitive personal data is not stored by PD
9	**How long will the information be retained for?** **- Align to the relevant retention periods.**	If register and not access the service = 2 years If register and access the service = until PD is informed that the patient is deceased, or patient closes their account If patients from surgeries not yet signed up register their interest = 1 year Consultation: Refer to GP Practice Privacy Notice
10	**What are the data formats?** **- Select only from list**	Registration: SMS, System Consultation: System

11	**If applicable, how is the information transferred / moved?** **- Select only from list**	Registration: System processing Consultation: System processing
12	**Who will have access to the data?** **- Specify with detail if known - individuals, teams, third parties or data processors etc.**	Registration: Bridlington PCN Care Navigator – HTFT clinical system Practice staff – HTFT clinical system PD Operational Staff – PD system only PD Medical Staff (inc Medical Officers) – PD system only PD Customer Experience – PD system only PD DPO – PD system only Consultation: PD GP's only who enter the data into EMIS or Sys1 - clinical systems which the patients GP will have access to

13	**How will access be restricted on a need to know basis?**	PD Operational staff are first point of contact for GPs and will not have access to consultation information PD Medical staff only have access to limited information – PD system or information retrieved from HTFT EMR's by Push Doctor's Medical Officers for purposes listed in the data sharing agreement. PD Customer Experience team can only access patient contacts and basic records from registration - they do not have access to information from the medical team or consultation – PD system only Consultation: Only PD GPs have access to write to the HTFT clinical system - no-one else in PD can access details of the consultation as it occurs PD GP's will also record high level information about the consultation as detailed in 3.1 of the data sharing agreement onto PD systems – access is restricted to those who need to provide treatment, employees with governance obligations and a limited number of employees responsible for healthcare operations

14	**What security measures will be put in place to protect the information, if known?**	Personal Data collected via the Platform is stored in secure environments that are not available or accessible to the public; only those duly authorised people, officers, employees or agents of Push Doctor who need access to information in order to do their jobs are allowed access. Anyone who violates our privacy or security policies is subject to disciplinary action, including possible termination of their contract with Push Doctor and civil and/or criminal prosecution Push Doctor uses the latest technologies to ensure utmost security, including utilising several layers of firewall security and encryption of Personal Data to ensure the highest level of security All users are required to go through a two-step verification process to create and restore an Account. Online access to an Account is protected with a password that a user creates which must meet the following requirements: Should be at least 8 characters long Should have at least 1 uppercase letter Should have at least 1 lowercase letter Should have at least 1 number Should have at least 1 special character and cannot contain '<' or '>' When using the Platform, all Personal Data are transmitted through the internet using Secure Socket Layers (SSL) technology. SSL technology causes a browser to encrypt entered information before transmitting it to our secure server. SSL technology, an industry standard, is designed to prevent a third party from capturing and viewing Personal Data Consultation: EMIS are compliant with ISO9001 for quality management systems ISO20000 for IT service management ISO27001 for information security Compliant with the Health and Social Care Information Centre (HSCIC) guidelines. Systm One cloud based provider - no details available

15	**Will this be solely automated processing (ie. is there no human involvement)?**	Registration: No Consultation: No
16	**Will any third parties or data processors involved?**	Yes
17	**List the processor (if existing relationship)**	No Processors used as part of the on-boarding process, but if a patient contacts PD Customer Experience team, we use Zendesk as a processor/application Microsoft Azure Cloud is also used by PD with servers located in the UK
18	**Geographic and / or logical location? (Where will the data be held)** **- Include if held by Push Doctor or third party such as a data processor or cloud services provider)**	Data provided directly to PD for registration and account activation is held within the UK within our own servers or through our cloud provider Microsoft Azure, in their UK South Servers. Data provided to the customer experience team through Zendesk may be held in the USA or EU. Zendesk has certified its compliance with the EU-U.S. Privacy Shield frameworks to the U.S. Department of Commerce and has been added to the Department of Commerce's list of self-certified Privacy Shield participants. Their certifications confirm that we comply with the Privacy Shield principles for the transfer of European data. As an alternative, Zendesk also have approved BCR (binding corporate rules) for the secure transmission of data across their Group. https://www.zendesk.co.uk/company/customers-partners/eu-data-protection/zendesk-chat/#content-
19	**Will the information be sent, stored or otherwise processed outside UK?**	Yes Zendesk may store data in the US as detailed in question 18

Section 4 - Risk Scoring:

	Section 4 - To be completed by DPO only.	
1	**List the possible lawful basis of processing**	Provision of service: Article 6(1)e - public task Article 9(2)h -healthcare and social care purposes Maintaining and improving the quality of service provided: Article 6(1)e - public task Article 6(1)(f) – legitimate interests Provision of information back to the Practice: Article 6(1)e - public task Article 9(2)h -healthcare and social care purposes
2	**Is the information being collected necessary and proportional for the intended purpose?**	Yes

3	**Identify and describe privacy risks to individuals** **(eg. excessive data collected, lack of transparency for data subjects, no legal basis for processing, data retained for too long, breach of confidentiality, data loss possible, accuracy, inability for individuals to exercise their rights, transfer outside of EEA without adequate safeguards)**	Registration: Data Sharing - risk that this may not transparent to patients using the service (low risk given that the service is being marketed as an extension to surgery and patients agree to a Push Doctor consultation before information is shared and are required to register with PD. Consultation: Systm One subject to an investigation by the ICO in Mar 2017 in relation to fair and lawful processing and data security. Commitment made in Aug 2017 to introduce new functionality to address Privacy concerns. Patients may request to update their sharing settings with the Push Dr GP. NB this is due diligence on the part of PD and responsibility lies with the GP practices using this system.
4	**Likelihood** **(Refer to risk rating guide)**	2
5	**Impact** **(Refer to risk rating guide)**	1
6	**Risk score**	2
7	**Is there a high risk to data subjects (red risk score) in the absence of mitigating measures and controls? This will require DPO consultation with the ICO.**	**no**

Section 5 - Risk Solutions:

	Section 5 - Only complete this section once the DPO has returned your PIA with Section 4 Completed	
1	**Describe the action / solution to address the risk**	PD's Operations Team will provide HTFT Practice Manager with at least 24 hour's notice of PD GP's requiring access to HTFT clinical systems to provide services as detailed in the DSA. They will provide the Doctor's name and smartcard number. When a PD GP no longer requires access to the HTFT clinical systems to provide the services as detailed in the DSA, PD will contact HTFT Practice Manager and inform them of the date that access should be revoked. The Practice Manager will review and confirm access with the PD's Operational Team on a 12-monthly basis. The Practice will deal with any specific requests to update a patient's sharing settings. Data sharing from PD to Practice is restricted to: Name DOB Mobile Email Consultation start and end time, duration Disruption reason if applicable Consulting GP details Cancelled appointments 'Did not attends' Patient feedback Data sharing is covered in the Privacy Notice Data sharing agreement will be in place and agreed by both parties as an addendum to the contract Data will be shared via secure SFTP
2	**Action owner**	Director of Risk and Governance, Push Doctor

3	**Target date for completion**	Go live

Section 6 - Accountability:

	Section 6 - To be completed by DPO only	
1	**Appropriate privacy notice?**	Yes
2	**Purpose limitation?**	Yes
3	**Accuracy?**	Yes
4	**Data minimisation?**	Yes
5	**Retention / Storage limitation?**	Yes
6	**Security?**	Yes
7	**Transfers?**	Yes
8	**Record keeping / Accoutability?**	Yes