THE WHITEHORSE PRACTICE

87 Whitehorse Road, Croydon CR0 2JJ,
Telephone 02086841162

BUSINESS IMPACT ANALYSIS

PIA (Privacy impact assessment screening questions)
These questions are intended to help organisations decide whether a PIA is necessary. Answering 'yes' to any of these questions is an indication that a PIA would be a useful exercise. You can expand on your answers as the project develops if you need to.

1. ***Will the practice collect new information about individuals? Will the practice compel individuals to provide information about themselves?***
   Yes when registering/when seeing a clinician

2. ***Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?***
   Yes (IT), New referrals i.e. hospitals & intermediate care

3. ***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

4. ***Does the practice use new technology which might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.***
   No

5. ***Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them?***
   Yes in terms of their health.

6. ***Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be particularly private.***
   Yes

7. ***Will the project require you to contact individuals in ways which they may find intrusive?***
   This is dependent on current circumstance.

Privacy Impact Assessment

The template follows the process which is used in the code of practice.

Identify the need for a PIA?

Personal data used within general practice for the purpose of referrals to hospitals and other intermediate services. Third parties to include:

- Social Services
- PICS – Personal Independent Co-ordinators
- Health Visitors for the Elderly/Children
- Community Pharmacists
- Croydon Respiratory Team (CRT)
- St Christopher's Hospice
- Residential or Nursing Homes

Explain what the project aims to achieve, what the benefits will be to the organisation, to individuals and to other parties. Also summarise why the need for a PIA was identified (this can draw on your answers to the screening questions).

Aim is to ensure all personal data is securely processed (including transferring data to other NHS Organisations) or held within the practice.

Describe the information flows (The collection, use and deletion of personal data should be described here and it may also be useful to refer to a flow diagram or another way of explaining data flows.)

- ***Access to medical records:***
  Practice receives request in writing.
  Staff have 5 days to provide patient with relevant information about online access however, copies of medical records will need to be sent to patient within 1 month.
- ***Third party requests:***
  Practice will obtain patient consent prior to sending/discussing personal information
- ***Registrations:***
  Patient requests for a registration pack.
  Once registration form is completed staff will check that all information required is provided.
  Id documents checked.
  The registration module on the practice clinical system is used to first check the spine for patient NHS number (if previously registered)
  Personal identifiable data is entered creating a record.

- ***Referrals:***
  GP consults with patient
  If a referral is needed GP will record on Dictaphone and pass to admin
  Admin will send referral via ERS, post, fax or email.
- *MDT's /Huddles*

Patient discussed as part of a multi- disciplinary team, discussion is taken as referral.

- ➢ Co-ordinate My Care:
  All palliative care patients as well as patients with complex needs will be entered on the website – Consent is obtained prior to entering on CMC website.

Practice list size: 7500
Number of Employees: 25

Explain what practical steps you will take to ensure that you identify and address privacy risks.

- ➢ Mandatory IG / Data Protection Training undertaken by all staff
- ➢ IG Policy in place and practice procedures in place
- ➢ Annual Risk Assessments
- ➢ Any risks Identified will be acted upon immediately and rectified
- ➢ Declaration of breaches or near breaches to ICO and CCG where appropriate

Who should be consulted, internally and externally?

- ➢ Senior Partner and Practice Manager
- ➢ ICO
- ➢ Croydon CCG

Identification of privacy and related risks:

a. Giving out of personal information which could identify the patient and be used maliciously, i.e. in phishing

b. Giving out medical information of patient to non-essential parties

c. Giving out practice staff personal information which could be used maliciously, i.e. identity theft

d. Giving out practice financial information without due cause

e. Allowing engineers or any other non-staff members access to secure areas without due cause with risk of theft of information or assets

f. Burglary during closing hours

g. Hacking of system information, i.e. medical, personal or financial

h. Use of non-encrypted disks, USBs or other portable data units

Identify privacy solutions
Describe the actions you could take to reduce the risks, and any future steps which would be necessary (e.g. the production of new guidance or future security testing for systems).

Result: is the risk eliminated, reduced, or accepted

Identification of privacy solutions; risk solutions; evaluation

a. Giving out of personal information which could identify the patient and be used maliciously, i.e. in phishing

Risk Solution

- Receiving and recording patient consent prior to giving out personal information

Result

- reduces risk of information used maliciously;

Evaluation

- impact of remaining risk is justified in managing patient care as per patient wishes

b. Giving out medical information of patient to non-essential parties

Risk Solution

- Receiving and recording consent prior to sending medical information to third parties, limiting amount of information to 'as needed' and information sent securely or collected by patient in person at reception

Result

- risk of information disseminated reduced on practice's part and only present in how patient and accompanying parties thereafter handle information

Evaluation

- impact of remaining risk is justified in managing patient care as per patient wishes

c. Giving out practice staff personal information which could be used maliciously, i.e. identity theft

Risk Solution

- Relevant staff member **only** to hand out their own information with exception of lawful reason for request, i.e. police inquiry

Result

- eliminates risk of information being used unlawfully

Evaluation

- impact on staff member is fully compliant to data protection law.

d. Giving out practice financial information without due cause

Risk Solution

- Only manager and Partners to hold access to and permission for usage of practice accounts

Result

- eliminates risk of unlawful usage of accounts

Evaluation

- is compliant and proportionate to data security laws

e. Allowing engineers or any other non-staff members access to secure areas without due cause with risk of theft of information or assets

Risk Solution

- All visitors to be signed in and out at guest book and to wear visitor id card visibly and to be lead into secure areas by member of staff so no security codes are given out unnecessarily

Risk

- this should eliminate risk of theft of information or assets

Evaluation

- measures taken are judges secure and proportionate

f. Burglary during closing hours

Risk Solution

- Building locked up and alarms set at end of day by reception staff with building keys and passcode limited to those who lock up in evening and open practice in morning plus CCTV

Risk

- this eliminates risk of burglary

Evaluation

- measures taken judged to be proportionate to security of practice

g. Hacking of system information, i.e. medical, personal or financial

Risk

- Up to date Mcafee firewalls, INPS and Window security systems, use of secure NHSmail and appropriate disposal of all obsolete data-holding hardware through CCG; reduces the risk of hacking;

Evaluation

risk remaining considered justified for purpose of managing patient care.

h. ***Use of non-encrypted disks, USBs or other portable data units and the use of anonymised and pseudonymised data***

Risk

- Use of non-encrypted devices and non-anonymised or pseudonymised personal data puts patient data at risk

Evaluation

- Only encrypted USBs used by practice staff and backups kept in locked area in manager's office. Practice uses anonymised and pseudonymised data therefore improving protection for data subjects, minimised risk when sharing data with processors or other data controllers. It also minimised the risk of data breaches.
- Risk of data reproduced unlawfully eliminated; proportionate measures taken to managing patient care securely.

Evaluation: is the final impact on individuals after implementing each solution as justified, compliant and proportionate response to the aims of the practice

Risk Assessed for current financial year?
Assessed for 2018-2019

Risks identified?
Risks identified: Smartcards left unattended and Screens not locked when staff are not at desk.

Implemented by?
Practice Manager

Risk Solution
Risk Eliminated

Action taken?

- ➢ Staff meeting GDPR discussed as part of the Agenda
- ➢ Risks identified are discussed and solution implemented
- ➢ Staff have been advised not to leave smartcards unattended, to remove when leaving desk.
- ➢ Screens must be locked each time a member of staff moves away from their desk
- ➢ Staff advised to refer to the practices' smart card policy and Clear Desk Policy

Integrate the PIA outcomes back into the project plan

Who is responsible for integrating the PIA outcomes back into the practice plan and updating any paperwork?

Milaine Borthwick-Ezekiel Practice Manager

Who is responsible for implementing the solutions that have been approved?
Milaine Borthwick-Ezekiel Practice Manager
Olivia Papics Administrator

Who is the contact for any privacy concerns which may arise in the future?
Milaine Borthwick-Ezekiel Practice Manager

Action to be taken Date for completion of actions:
The practice is found to be compliant for the year 2019-2020

Signed off by: Milaine Borthwick-Ezekiel (Practice Manager/ IG Lead) Date: 28/03/2019

Annex three

Linking the PIA to the data protection principles
Answering these questions during the PIA process will help you to identify where there is a risk that the practice will fail to comply with the DPA or other relevant legislation, for example the Human Rights Act.

Principle 1

- Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:

a) at least one of the conditions in Schedule 2 is met
b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

- ***Have you identified the purpose of personal data collection?***
  Yes health and or social services

- ***How will individuals be told about the use of their personal data?***

  During a consultation with a clinician or via letter to patients

- ***Do you need to amend your privacy notices?***

  No, notices are relevant and up to date

- ***Have you established which conditions for processing apply***?

  Registrations, Referrals, MDT's, SCR, Online Access

- ***If you are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or withdrawn?***
  - ➢ Write to the patient to come in and sign a consent form.
  - ➢ Consent or Consent declined is recorded on patient's notes.
  - ➢ If withheld or withdrawn third parties will be informed in writing.

If your organisation is subject to the Human Rights Act, you also need to consider:

Will your actions interfere with the right to privacy under Article 8*?*

- ***Have you identified the social need and aims of the practice? Are your actions a proportionate response to the social need?***
  Staff have been advised not to access personal data for social purposes, failure to adhere to the practice policy can result in disciplinary action taken by the practice.

Principle 2

Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

- ***Does your practice plan cover all of the purposes for processing personal data?***
  Yes our plan covers the following:
  - ➢ Registration
  - ➢ Referrals
  - ➢ SCR
  - ➢ Online access to appointments and prescriptions
  - ➢ Multidisciplinary Meetings to include Social Services, District nursing Team, Community Matron, Health Visitor for the Elderly, Mental Health Team
  - ➢ Co-ordinate my care & St Christopher's Hospice, Croydon Respiratory Team/ Rapid Access Chest Clinics/ TAC's
  - ➢ Staff Smartcards : Personal information required to verify ID
  - ➢ DBS Checks: Staff personal information required

- ***Have potential new purposes been identified?***
  Yes: Huddles / Dermatology App

Principle 3

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

- ***Is the information you are using of good enough quality for the purposes it is used for?***

  Staff will ensure that the data collected is adequate, relevant and not excessive in relation to the purpose for which they are processed.

- **Which personal data could you not use, without compromising the needs of the practice?**
  It is dependent on what information is required, staff to provide only what is required, no more.

Principle 4

Personal data shall be accurate and, where necessary, kept up to date. If you are procuring new software does it allow you to amend data when necessary?

The practice uses the INPS Vision clinical system which allows practice staff to update and amend data when necessary.
All data is secure and kept up to date.
Paper medical records are stored in the "Records Room" which is permanently locked; keys are kept in practice manager's room.

How are you ensuring that personal data obtained from individuals or other organisations is accurate?

Staff will contact the patient/organisations to authenticate the information received.

Principle 5

Personal data processed for any purpose or purposes shall not be kept for longer than necessary for that purpose or those purposes.

- ***What retention periods are suitable for the personal data you will be processing?***

  Retention periods do not apply to general practice.
  All patient data is stored indefinitely or until transfer to another medical practice or in the event of death.

In the event a patient has transferred to another GP practice, medical notes are either sent via GP to GP via secure link and/or paper versions are transferred via the PCSE secure courier service

- Are you procuring software which will allow you to delete information in line with your retention periods?

Principle 6

Personal data shall be processed in accordance with the rights of data subjects under this Act.

- ***What systems are in place for patient's requesting access to their medical records and does the practice procedure allow staff to respond to subject access requests more easily?***
  Staff are aware requests for access to medical records are to be accepted only if received in writing.
  All written requests must be responded to within 5 working days
  Practice procedure for patient access to medical records allows staff to respond in a timely manner

- ***Is there a procedure for individuals to opt out of their information being sent to third party organisations?***
  Yes there is provision for patient to opt-out.

  9Ndg: Consent given to share patient data with third party

  9NdH: Decline consent to share patient data with third party

  9NdJ: Consent withdrawn to share patient data with third party

Principle 7

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

- ***Do any new systems provide protection against the security risks?***
  Anti-virus has been installed on all computers and is updated once a year.
  GP systems are monitored by NELCSU

- ***What training and instructions have been undertaken by staff?***
  All staff have completed the Data Protection / GDPR course by Croydon CCG and E-learning course on NHS Data Security online

Principle 8

Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country of territory ensures and adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. Will the project require you to transfer data outside of the EEA?

- ***If you will be making transfers, how will you ensure that the data is adequately protected?***

  Patient consent is obtained and recorded,
  Data set to be transferred is encrypted prior to being sent