Data Protection Impact Assessment Report

Practice name	**Park View Group Practice**
Data controller	**Amy Waters**
Date of assessment	**15/11/2018**
Process assessed	**Viaduct clinical staff accessing the clinical system to record consultations with patients**

Overview:

Park View Group Practice currently adheres to internal policies and national legislation and guidance for all processes that involve personal data. To ensure that the practice is compliant with the GPDR, a review of all processes is being undertaken.

The need:

Having completed Step 1 of the DPIA, when asked "Does the process involve any of the following", this question merited a "yes" response:
"The sharing of data subjects' health information between organisations"

The practice is frequently required to share data subjects' personal data – more specifically, personal details and healthcare between organisations. That is the sharing of data between Park View Group Practice and Viaduct Healthcare Professions in this case. This is a requirement to ensure that data subjects receive the necessary care and treatment commensurate with their clinical condition(s).

Assessing the risk:

Information collection – Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject	
What information is being collected and how?	**Patients symptoms warranting an appointment with the member of the clinical team**
Where is the information being collected from and why?	**From the patient directly**
How often is the information being collected?	**At appointments, the Physiotherapists are in three days per week, and the Well-being Navigator and Pharmacist one day per week**
Information use – Is the data obtained for specified, explicit and legitimate purposes?	
What is the purpose for using the information?	**To enable the provision of effective healthcare treatment**

When and how will the information be processed?	**Recorded during consultations onto the EMIS Web clinical system**
Is the use of the information linked to the reason(s) for the information being collected?	**Yes**
Information attributes – Personal data shall be accurate and, where necessary, kept up to date	
What is the process for ensuring the accuracy of data?	**Asking the data subject to confirm details and ensuring the correct patient record is used when recording the information**
What are the consequences if data is inaccurate?	**Incorrect patient record updated; delay in treatment and or referral; potentially adverse impact on patient health**
How will processes ensure that only extant data will be disclosed?	**Only that information which is pertinent to the referral will be used; this is extracted onto medical templates using the IT system**
Information security – Personal data shall be processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures	
What security processes are in place to protect the data?	**Only authorised users can access the data. Staff must adhere to the NHS policy for the use of IT equipment**
What controls are in place to safeguard only authorised access to the data?	**Regular audits of access to healthcare records. All users have an individual log-on and the system is password restricted**
How is data transferred; is the process safe and effective?	**Data from the consultation will only be transferred electronically if a referral is required to another healthcare organisation**
Data subject access – Personal data shall be accurate and, where necessary, kept up to date	
What processes are in place for data subject access?	**Data subjects can access limited information using online services or by submitting a SAR**
How can data subjects verify the lawfulness of the processing of data held about them?	**By accessing their records and viewing how information has been processed**
How do data subjects request that inaccuracies are rectified?	**Data subjects can request that information held about them be**

	changed by asking for an appointment with the data controller
Information disclosure – Personal data shall be processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures	
Will information be shared outside the practice; are data subjects made aware of this?	**Yes, the practice privacy policy details this information**
Why will this information be shared; is this explained to data subjects?	**Yes, to facilitate the necessary examination and treatment of data subjects**
Are there robust procedures in place for third-party requests which prevent unauthorised access?	**Yes, authority must be provided by the third party who also included either a written statement or consent form, signed by the data subject**
Retention of data – Personal data shall be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed	
What are the retention periods associated with the data?	**GP records are retained for a period of 10 years following the death of a patient**
What is the disposal process and how is this done in a secure manner?	**At the end of the retention period the records will be reviewed and if no longer needed then destroyed**
Where is data stored? If data is moved off-site, what is the process; how can data security be assured?	**Patient data is stored electronically on the IT system (EMIS Web) and hard copies of patient records (if held) are stored in the reception office, which can only be accessed by authorised personnel**

To assess the risk of this process, this risk matrix was used:

Probability	Severity of Impact/Consequences			
		Minor	Moderate	Major
	Frequent	Medium	High	High
	Likely	Low	Medium	High
	Remote	Insignificant	Low	Medium

The risk for this process has been recorded in the risk register, which details the mitigating actions taken to reduce the risk.