PatientChase DPIA

(Data Protection Impact Assessment)

Controller Details

Name of controller	General Practice Software Solutions
Subject/title of DPO	miles.dagnall@jem.gdpr.co.uk
Name of controller contact /DPO (delete as appropriate)	Miles Dagnall

Need for a DPIA

Introduction

PatientChase is a solution developed by GP Software Services an EMIS Web accredited partner. Our product simplifies and automates all aspects of patient recall, enabling a primary care unit such as a GP practice to identify patients, communicate with them and code all contacts made.

PatientChase helps practices save money, improve efficiency and ultimately improve the quality of care provided to patients. It will call in patients the least number of times necessary, providing greater convenience for them whilst helping to improve surgery access. It can also be used to

In order to follow best practice for protecting patient data, PatientChase has adopted a "privacy by design" approach. This Data Protection Impact Assessment has been produced to assess the risks of an organization working with us as a third party data processor.

However, it is the responsibility for any organization acting as a data controller to construct its own Data Protection Impact Assessment.

Description of Processing

When employed by a practice, for example, PatientChase extracts data from EMIS during a synchronization, so can be described as an off-line reader. This data is imported into an encrypted database with AES256bit encryption which sits on the local host machine or a local shared drive. PatientChase then accesses information which marries contact patient identifiable data with their associated recall data based on their conditions for calling them in to see clinicians in a combined clinic. PatientChase contacts patients via SMS, letter, emails and provide spreadsheets for telephone contact as a back-up.

PatientChase also records all media sent out to patients and files media back into EMIS with the associated Snomed code to help the audit trail. This audit trail remains within practice systems.

By automating recall and merging outstanding targets into one list which is patient based the patients need fewer practice appointments at less frequent intervals and there is less demand on GP services as a result. This saves appointment time making significant financial savings and space for better targeted patient care.

Any dead or patients who have left the practice are removed from the database during the sync.

Personally Identifiable Data remains at all times on the Data Controller's system. Personally Identfiable Data is not disclosed by GP Software Services to any third party. PatientChase extracts only anonymized data for contractual and system management purposes.

PatientChase is an approved EMIS programme partner.

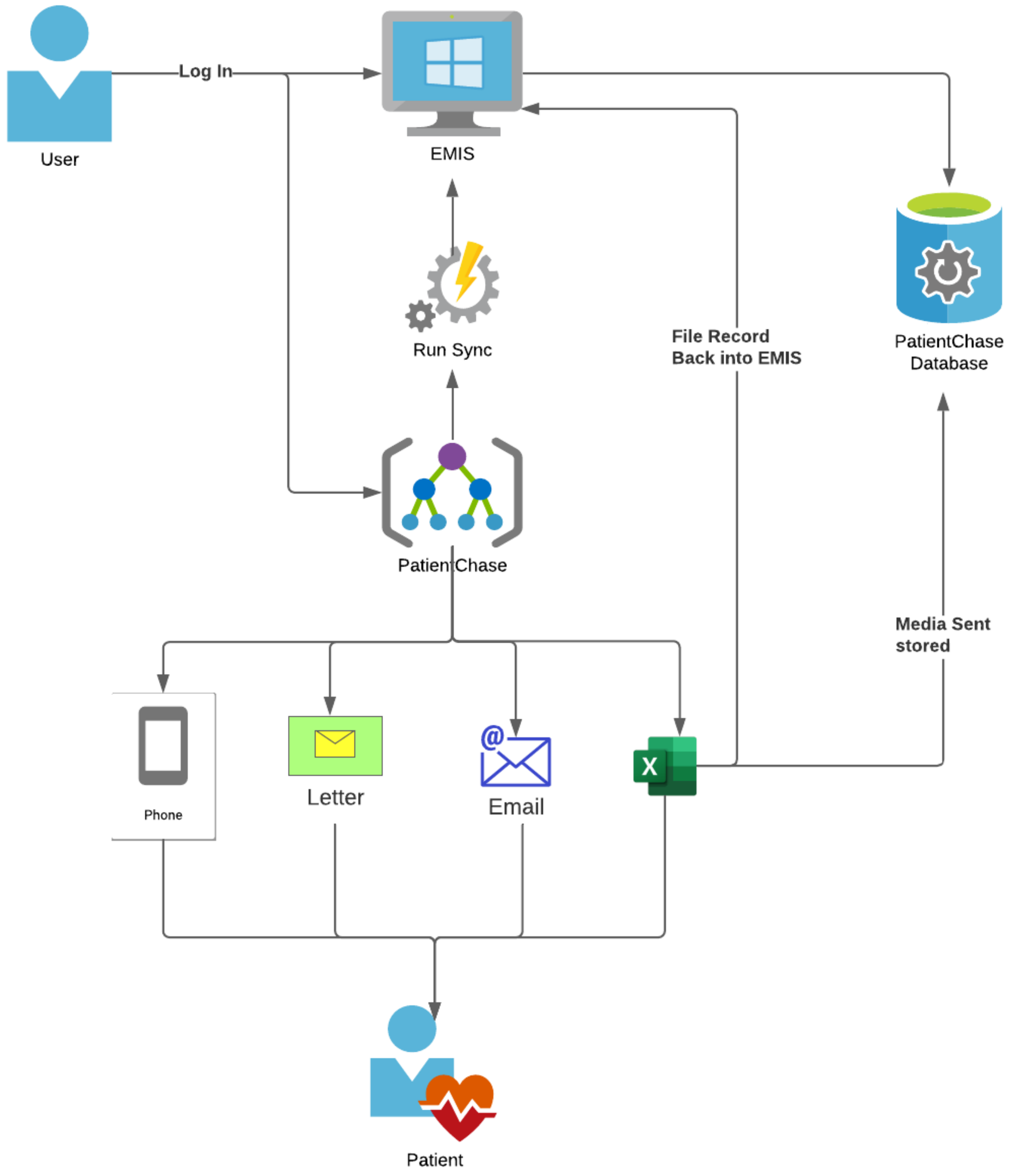
PatientChase is an NHS Business Partner and therefore meets the same Information Governance requirements as NHS organizations including the annual completion of the Data Security and Protection Toolkit. Confirmation can be found on the NHS Digital Website at https://www.dsptoolkit.nhs.uk/OrganisationSearch.

GP Software Services are also registered with the Information Commissioner’s Office, has a Senior Information Risk Officer and a registered, independent, Data Protection Officer who monitors compliance with the 2018 Data Protection Act (GDPR) and advises on complaints.

Purpose of the processing

The purpose of the processing is to help the surgery to contact the patient in the most suitable way possible in order to improve their health care. This has patient benefits to help with prevention and control of long-term conditions which will help patients live a healthier life and will benefit the surgery financially via their target driven pay outcomes.

The processing and the data flow



The Data Controller user logs in using their username and password via the EMIS API. They can also autologin to EMIS and, when running PatientChase, this will also autologin. No log-in details or passwords are ever stored into PatientChase.

When they run a sync information is extracted from EMIS and pushed into the PatientChase Database. Once the sync is complete, searches can be created which merge predefined targets and lists views in a grid within PatientChase, showing both the patients and any outstanding medical targets needing action .

The user then has the option to send the patient a reminder via various forms of media and record this back in to PatientChase and within the PatientChase Database

PatientChase can run reports of patient contacts with the particular media used to make contact.

Context of the processing and legal basis

The context of the processing is in line with generating demand for proactive care of the patients and to case find patients who have outstanding targets who need to come in for a review. They can be contacted via a variety of various media types to help improve compliance and reduce DNAs.

As this may be a new system for many Data Controllers, they will need to decide what the legal basis will be for processing patient data and whether a Data Protection Impact Assessment is required.

This Data Protection Impact Assessment may be used to assist the Data Controller in the construction of their own.

Typical legal bases that are used in primary care for this kind of processing are:

Article 6(1)(e) '…the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority…'.

Health data is defined as a special kind of personal data and is also processed by the practice under

Article 9(2)(h) 'necessary for the purposes of preventative 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..'

Consultation process

Consultation with relevant stakeholders

During the scoping of the Data Controllers requirements our approach is to make ourselves consistently available to recall leads and other relevant clinicians and administrators so as to involve them with the processes within PatientChase, to make them aware and to provide assistance with the dataflow and how it works best within a practice or any other primary care unit. Our assistance extends to helping with any Data Privacy or Information Governance issues.

Security Measures

Technical Security Measures

PatientChase extracts data from EMIS during a synchronization, so can be described as an off-line reader. This data is imported into an encrypted database with AES256bit encryption which sits on the local host machine or a local shared drive.

PatientChase meets the standards of the NHS Data Security and Protection Toolkit.

Organizational Security Measures

All PatientChase staff are under obligations to maintain patient confidentiality. However the system has been designed so that staff do not have access to Personally Identifiable Data of patients.

Staff will take NHS related information governance training on appointment and annually thereafter.

Data Controller staff, typically, will access the system only through their normal secure EMIS log-in processes.

Possible Risks

Describe source of risk nature of potential impact on individuals and mitigation.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high
Patient Data may be revealed or downloaded to an unauthorized third party PatientChase is a view of patient data that remains wholly within the Clinical System and remains within the Data Controllers' systems. GP Software Systems does not have access to PID.	Remote	Signiificant	Low
Patient data could be sent to an incorrect patient PatientChase is dependent upon the accuracy of the data within the Clinical system and this risk is outside of the control of PatientChase.	Remote	Significant	Medium
	Possible	Significant	Medium
Patients not picked up on the searches during the sync Values not correctly picked up on EMIS synchronizations. PatientChase has been subject to rigorous testing programme to eliminate this risk.	Remote	Significant	Low
(Please note that these risks are designed as indicative only -Data Controllers must make their own risk assessment)			

Mitigations for Reducing Risk

Identify additional measures Data Controllers could take to reduce or eliminate risks identified as medium or high risk as above.

Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
		Eliminated reduced accepted	Low medium high	Yes/no
Sent media to Wrong Patient	GP surgery to ensure all demographics are up to date and for the intended patient. This is the same as even if PatientChase was not used	Accepted	Low	Yes
Patients Not Picked up in the sync	PatientChase is very flexible in it's ability to adapt the specific snomed codes as used within the Primary Care Unit (Practice). It is advised that a test synchronization is carried out to ensure that relevant codes are being picked up.	Accepted	Low	Yes

Sign Off

Item	Name/position/date	Notes
Measures approved by:		
Residual risks approved by:		
DPO advice provided:		
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:		The DPO should also review ongoing compliance with DPIA