Primary Care Sheffield Data Protection Impact Assessment

1. Document Change History

Version	Date	Author	Reason
V1.0	03/03/2023	Thomas Eyles, 6B	First draft
V1.1	27/09/2023	Thomas Eyles, 6B	Final Amend
V2.0	14/05/2024	Thomas Eyles, 6B	Amends as per TPP guidance
V2.1	06/06/2024	Thomas Eyles, 6B	Amends as per TPP guidance

2. Purpose of the DPIA

The purpose of this Data Protection Impact Assessment (DPIA) is to assess the potential risks associated with the processing of Patient data and to identify measures to mitigate those risks. The assessment is conducted in compliance with relevant data protection laws and regulations, including the General Data Protection Regulation (GDPR).

Scope

This DPIA covers the processing of Patient data within the PCS application.

Data Controller and Processor Information

- Data Controller: Primary Care Sheffield
- Data Processor: 6B Digital Ltd

3. Project Summary

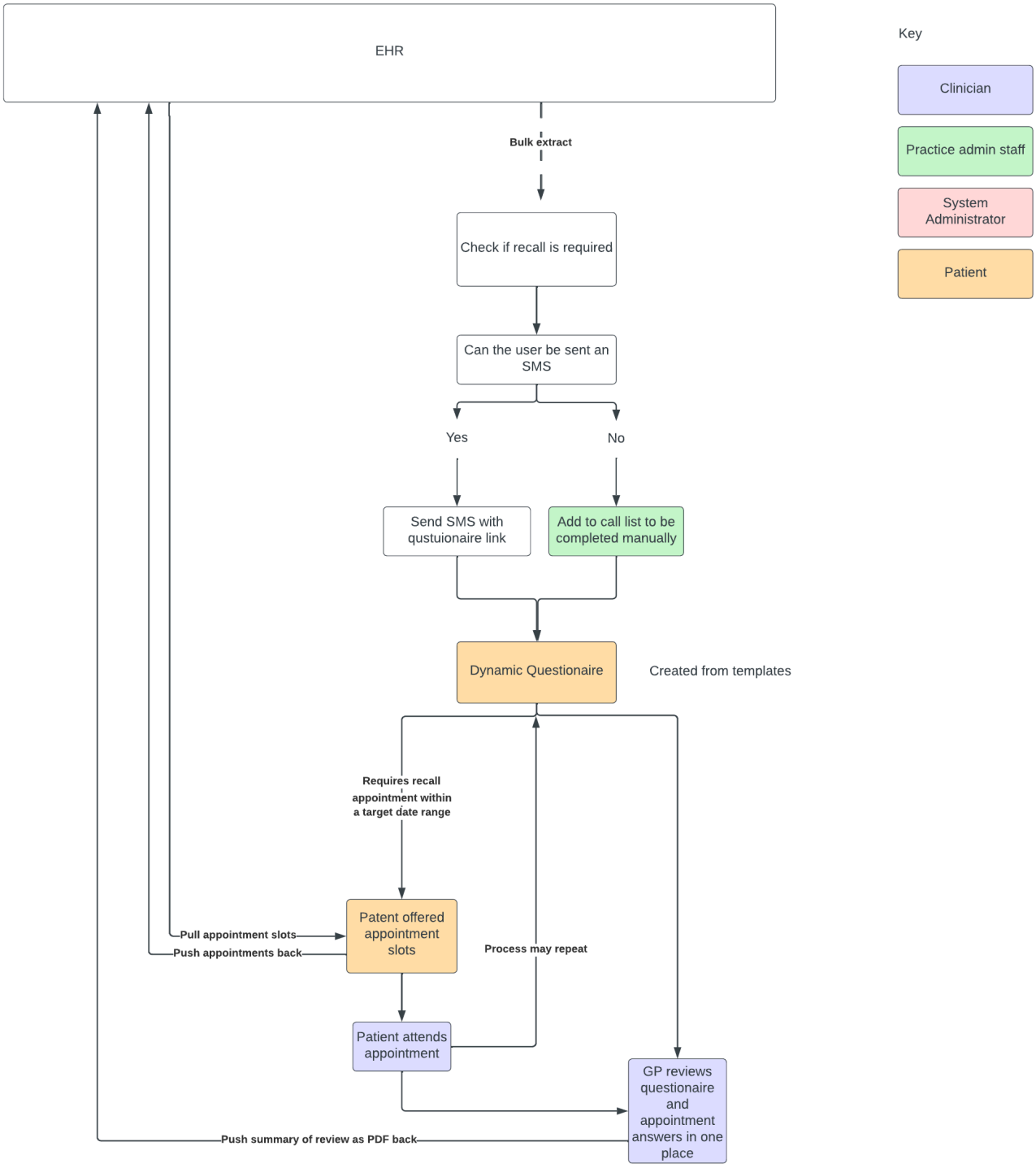
Primary Care Sheffield (PCS) are looking to build a web and desktop application to assist GP practices in the management of patients with long term conditions. The PCS platform will look to improve the patient journey through their review, by sending them a questionnaire via SMS or email that contains their relevant recall.

Furthermore, the PCS platform will look to relieve the pressure on the NHS and the current staffing problems it faces, by assigning appointments to the relevant skill set required and to cut down on the number of appointments, by combining reviews/appointments.

Practice staff members will also be able to better track against QOF targets, which will look to increase the financial advantages for a practice.

The purpose of completing this DPIA is to have a framework in place to cover Primary Care Sheffield as sensitive personal data will be stored.

Below is a diagram that depicts the user flow through the PCS platform.



4. Data Processed

Summary

The data is collected by PCS is directly from the electronic health records systems, EMIS and SystmOne (Providers) through a bulk extract service, provided by the electronic health record suppliers every 24 hours. The data is provided in encrypted files over a sFTP connection, which is then securely stored in a PCS FHIR service datastore. All encryption keys are stored in a UK datacentre in a access controlled environment.

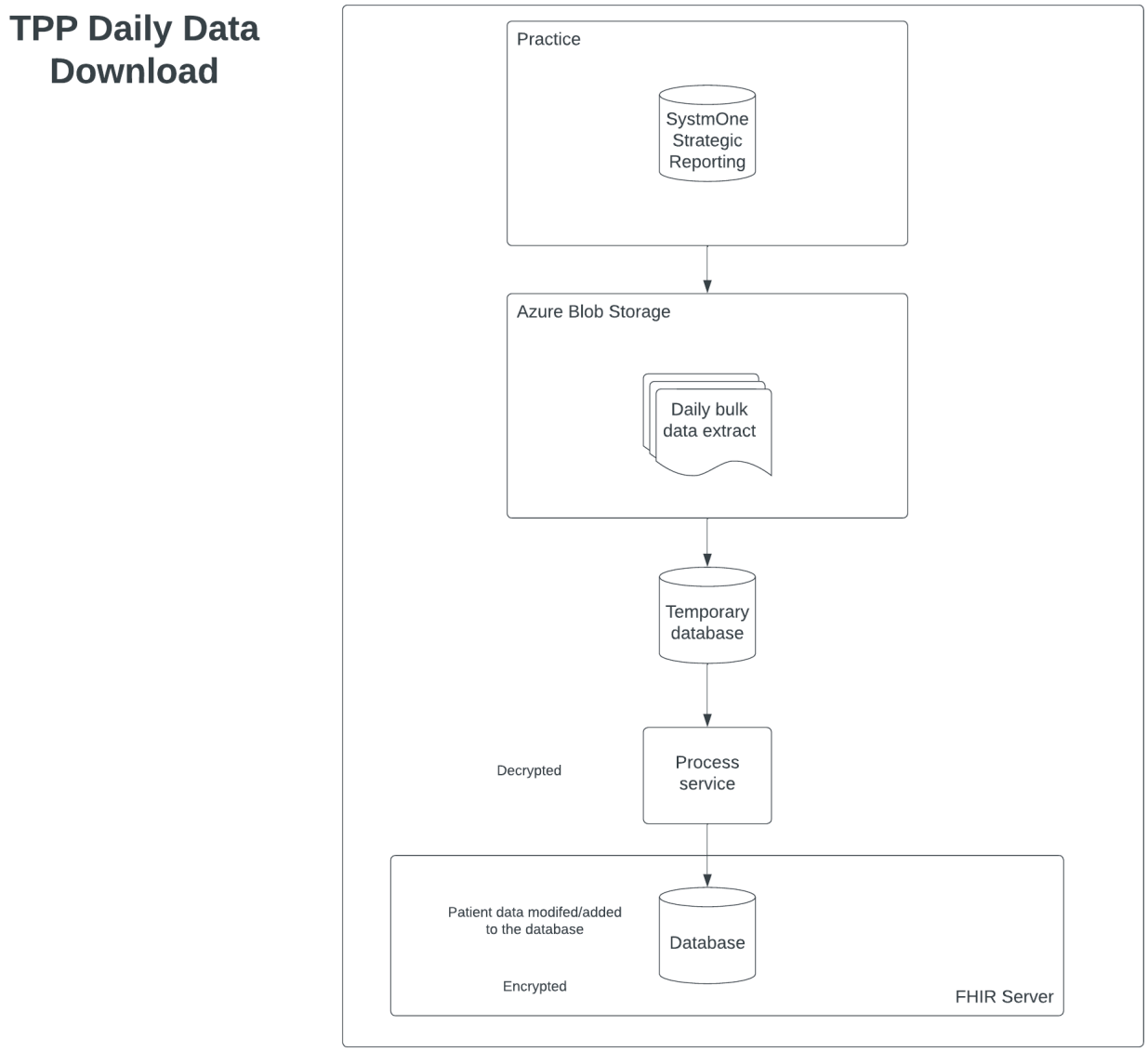
As the application is storing sensitive personal information in a FHIR server on Azure, all data is encrypted at rest. No data is supplied from the PCS datastore to other applications.

In order for Primary Care Sheffield to receive patient data:

- a valid data sharing agreement must be in place between PCS and a practice
- a PC must be running as a gateway to the application

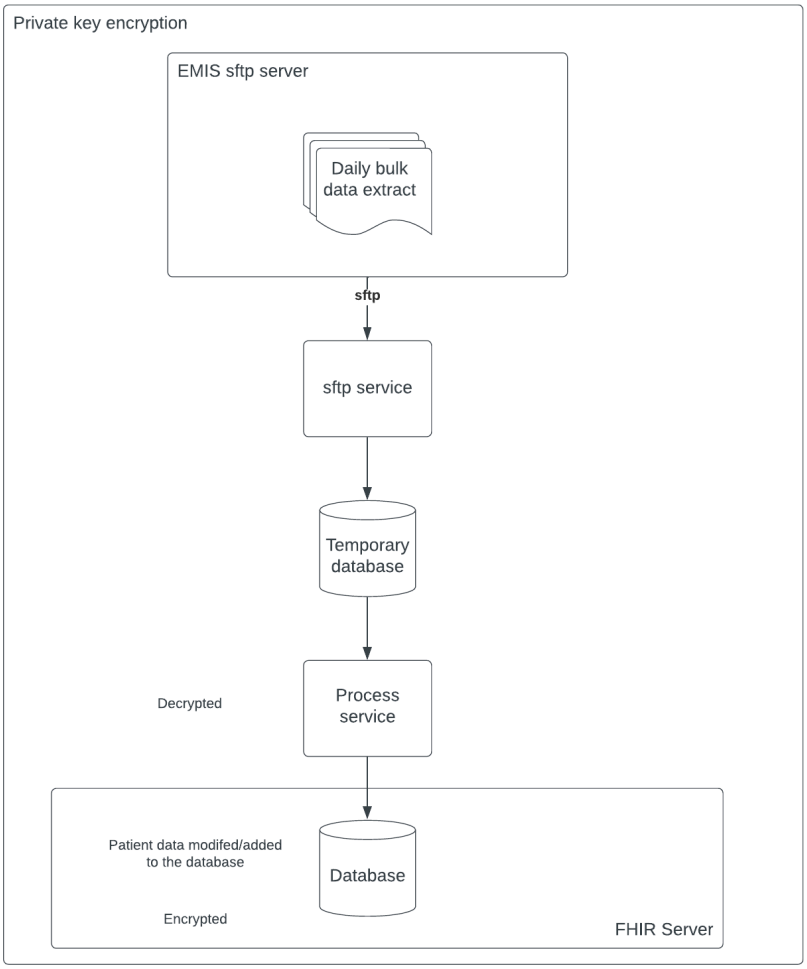
Described Data Flow

SystmOne Data Flow

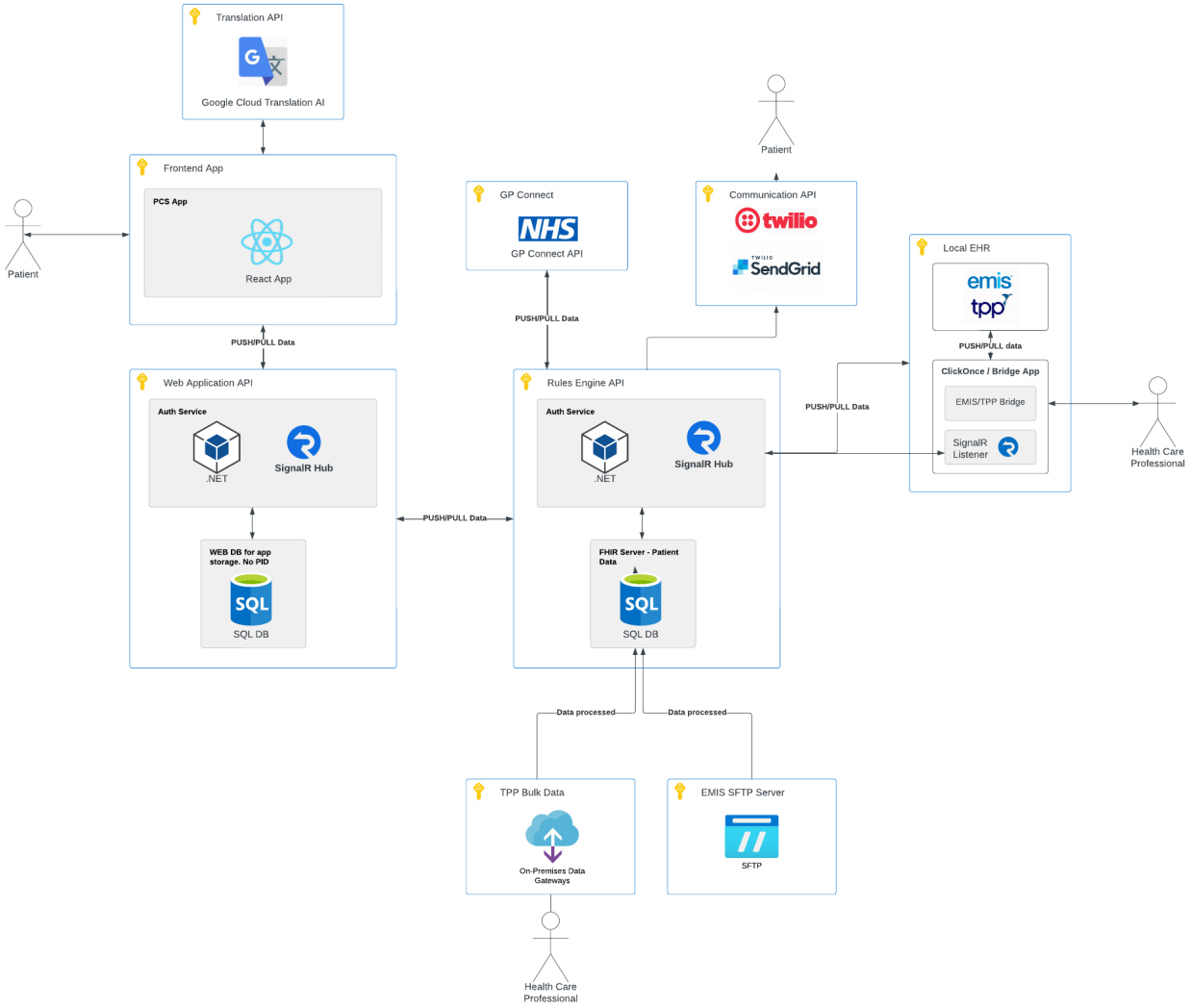


EMIS Web Data flow

EMIS Data Flow



PCS System Architecture



Data Defined

Data will be provided daily via the Providers, first as a bulk extra, then as daily delta updates that only contain new updates on a chosen patient.

The geographical areas covered will be determined by the data sharing agreements in place with PCS and their clients, and will then affect all patients in that area that have their data sharing settings enabled.

All patients and their data are extracted by PCS, only data that is marked as confidential or deleted by the provider will not be extracted. PCS require all patients in their local data store to assess whether they require care through the PCS platform. PCS will look to minimise the data stored against a patient by only extracting the relevant and required data, this includes:

Data Type
Patient first name
Patient last name
Patient middle name
Patient gender
Patient address
Patient phone number

Patient email address
Patient date of birth
Patient NHS number
Patient problems
Patient medication & prescriptions
Patient test results
Patient consultations
Healthcare professional name
Healthcare professional email
Healthcare professional role
Healthcare professional workplace

Data Context

The data stored in the PCS platform is aimed at better providing long term care for patients with ongoing conditions/prescription drugs. The patients in the PCS platform will include children and patients of a vulnerable group. A patient or GP can mark a patient as confidential, to remove them from the PCS platform. Steps have been made in the PCS platform to ensure that any patient of a vulnerable nature is communicated in a appropriate way, through a designated guardian.

All of the data processed by PCS is covered under a data sharing agreement with an individual practice or primary care network and will be used in a lawful and method that is intended for use.

There are risks associate with the transfer and processing of patient data. For this reason as part of the validation process with the Providers a full threat model with threat mitigations was produced. All mitigations, such as encrypted transfer, were implemented into the software. As per GDPR where possible data is minimised and retained only for as long as required to complete the required task. PCS as an organisation is also ISO27001 and NHS DSP Toolkit compliant, this further ensures if future risks are identified and accepted practices are used to capture, investigate and fix any issues

Child Data

Children data will be extracted and used in the PCS platform, including demographic and immunisation data. This is to improve the recall activities for child patients with long term conditions and their child immunisations.

Special Category Data

Special category data stored:

- ethnicity
- health data

This data is stored to ensure that each patient is sufficiently and correctly categorised in order to receive the most suitable care. This is used in the patient recall algorithm to determine whether the outcome/monitoring required is different due to special category data. An example might be, a patient on X medication with X condition and of X ethnicity must be sent X questionnaire (questionnaires are built in the system).

5. Identifying and Mitigating Risks

Data quality

An individual patient record is created using their NHS number as the single unique identifier. Duplication of patients is avoided by using the NHS number as a unique identifier. As part of the separation of responsibilities in the Joint Controller agreement, Providers are responsible for the quality of data they provide to the PCS platform. Where PCS act as a Sole Controller, patients can upload their own symptoms and monitoring figures. This data is flagged to clinicians as part of their review, so that clinicians can make more informed decisions.

Security assessment

The PCS platform is hosted on UK-based Cloud servers and undergoes annual penetration testing by an accredited company commissioned by PCS. This includes a follow-up test to review changes implemented since the initial test. This will be implemented before the initial launch in June 2023, with the follow-ups planned for June 2024. Backups are also held on UK-based Cloud servers.

A application-level threat modelling has been carried out to identify and mitigate against potential application vulnerabilities. This has been carried out prior to development and aims to provide prevention methods against common attacks, including credential stuffing, brute force and other injection/scripted attacks.

Compliance risk - UK GDPR article 5(2): Accountability

As Controller and Joint Controller, all parties involved in processing have responsibilities around their compliance with the principles of UK GDPR. These are reviewed below to ensure that PCS has evidence to demonstrate compliance with each.

1. Personal data must be processed lawfully, fairly and in a transparent manner
   Where PCS act as Controller there are clear lawful basis under UK GDPR Article 6 to process personal data and exemption to process special category personal data (UK GDPR Article 9).
2. Only use personal data for specified purposes
   PCS only use personal data for the purposes of managing a patients long term condition where there is lawful basis to do so. PCS do not use the personal data for any commercial purposes, nor do they sell any of the personal data.
3. Only use the minimum necessary personal data
   The PCS platform holds personal data about patients transferred to the platform by Provider organisations. The Provider organisations have the responsibility for ensuring only necessary data is sent to the platform.
4. Ensure data are accurate and up to date
   Providers have the responsibility to ensure that data they send to the PCS platform is kept accurate and up to date. Data is cross referenced at different intervals of a review stage, via the Providers transactional APIs to ensure that it is as up to date as possible when judgements/recommendations are required.
5. Only keep personal data for as long as necessary
   The retention of the Personal Data with the PCS platform is kept in line with the NHS Records management Code of Practice and to ensure continuing access to that information, both for care purposes, and for related purposes involving such matters as audit, complaints handling, and litigation. This is a period of 8 years.

PCS maintains a high level of security of its data in both a technical and organisational manner. This includes encryption so that although PCS is a Controller for this data, they are unable to access this data internally aside for the management of the record. Only a practice user will be able to access patient data, that pertains to them.

6. Sign off and record outcomes

Item	Name/date

DPO advice provided:	Caroline Million, 15/03/2023
Summary of DPO advice:	Approved
This DPIA will be kept under review by:	Automotive Healthcare Ltd