iPlato Connect & myGP

Information Governance (IG) FAQ

iPlato Healthcare Ltd

October 2024

Version 2.5

iplato
a HUMA company

Contents

ABOUT THIS DOCUMENT

This document provides detailed information pertaining to the iPlato Connect platform which includes iPlato Connect, iPlato Toolbar and the myGP App.

The information provided within this document may be revised from time to time and will be updated in line with new legislative requirements and/or updated product features and additional services at the sole discretion of iPlato.

The document is not intended for general circulation; it provides iPlato Connect platform customers and users with guidance on interpreting the UK GDPR within the healthcare space, specifically in relation to iPlato Connect products and services.

This document supersedes any prior documents or written policies of iPlato that are inconsistent with its provisions.

Questions, comments and requests regarding this document should be addressed to:

iPlato Healthcare Ltd
Millbank Tower
21-24 Millbank
London
SW1P 4QP
ig@iplato.com

Version Control

Version	Release Date	Comment	Approver
1.0	December 2012	Initial release	M Rowden
1.1	November 2016	Updated and split into separate docs	M Rowden
1.2	January 2017	Updated logo and management review	M Rowden
1.3	June 2017	Updated to FAQ style, additional content	M Rowden
1.4	June 2017	Addition of Appendix I – NHS guidance	M Rowden
1.5	Aug 2017	Modification to align to GDPR	M Rowden
1.6	Sept 2017	Clarification of Data Sharing guidelines	M Rowden
1.7	Sept 2017	Revised GDPR guidance	M Rowden
1.8	Aug 2018	Revised GDPR	M Rowden
1.9	Oct 2019	Refreshed content, added DPIA example answers	M Rowden
2.2	July 2020	Refreshed content; combined GP & CCG versions	M Rowden
2.3	March 2022	Review and extensive revision (eg: including Risk section and updating UK GDPR references)	M Rowden
2.4	October 2022	Add legacy Patient Comms info & ISO accreditations	M Rowden
2.5	October 2024	Refreshed hosting/security details and product terminology – general review / revisions	M Rowden

INTRODUCTION

Handling & Processing of Patient Data

Since the initial development of myGP Messaging back in early 2003, iPlato has ensured that the security and confidentially of patient data were at the centre of the design of the system. Accordingly, iPlato strives to adhere to the stringently set requirements of the (now UK) General Data Protection Regulation and the Data Protection Act 2018 as well as guidelines imposed by NHS England, clinical system providers and client Trust Caldicott Guardians.

Additionally, iPlato must ensure compliance with NHS Data Guardian Standards generally as well as specific requirements as mandated to maintain an approved NHS Data Security and Protection Toolkit accreditation, which is a mandatory requirement to support a direct connection to the NHS HSCN network.

Why is IG Important?

Information Governance has a number of fundamental aims:

1. To support the provision of high-quality services by promoting the effective and appropriate use of information.
2. To comply with all relevant legislative requirements thereby protecting individuals, the company and its employees.
3. To manage the creation, storage, movement and sharing of data in a secure and efficient manner.
4. To encourage responsible staff to work closely together, preventing duplication of effort and enabling more efficient use of resources.
5. To develop support arrangements and provide staff with appropriate tools and support to enable them to carry out their responsibilities to consistently high standards.
6. To enable the organisation to understand its own performance and manage improvement in a systematic and effective way.

The iPlato Approach

iPlato is committed to continued innovation in health services to support GPs, ICB's, PCN's and patients but strongly believes that this can never be at the expense of the protection of the data upon which such innovations depend. Patient safety and Information Governance is at the centre of everything we do. All of our products and services are developed to meet or exceed best practice in information governance and data protection concerns.

It is particularly important to us that everyone is clear how data is used. We have therefore prepared this FAQ to answer the key questions around data management and compliance. iPlato offers several different services. The way in which patient and other data is collected varies between them. We cover each separately below. A general overview that applies to both iPlato Connect and myGP App services is set out in Section 1 - General.

FAQ

Section 1 – General

What are the fundamental differences between iPlato Connect (inc. Toolbar) and the myGP App and how does this impact patient data?

iPlato Connect and its associated modules is a cloud-based middleware platform securely hosted within the HSCN (formerly N3 network) and integrated directly with NHS approved clinical systems. It is procured and used by NHS organisations (eg GP's, ICB's, Public Health). It has a variety of functionalities/features that include data messages, user Toolbar, patient questionnaires, video messaging, self-book, patient triage, friends and family tests.

From a data protection perspective, iPlato Connect GPs [and/or other relevant NHS stakeholder organisations, eg ICB's] remain as Controllers. iPlato is a Processor and simply processes the personal data of patients to provide the service to the NHS organisations.

myGP is an App developed for the exclusive use of patients and it is provided for and available to all UK registered patients. It is provided free of charge and distributed directly to patients by iPlato through the Android and Apple App stores. GP's, ICB's or other NHS bodies have no capacity to influence, restrict or control access to the App for any patient. The App is integrated directly to the patients' medical records (via official and NHS assured API's). Additionally, the App contains features that collect and process patient generated data, patients provide explicit consent for this when entering data in the App.

From a data protection perspective, iPlato is a Processor in respect of GP clinical system sourced data and a Controller in respect of patient generated/collected data. Where patient generated/collected data is subsequently shared with NHS / Healthcare organisations, iPlato is the Controller for such sharing and ensures explicit patient consent is provided.

What is iPlato's 'Privacy Policy' with data subjects?

Please see the iPlato Privacy Notice which is published here: [Privacy Policy - iPLATO]()

This provides information to data subjects as to how iPlato will process their personal data when they use the iPlato website or other iPlato products/services excluding the myGP App*. Users of the myGP App are informed by the specific terms of the App Privacy Policy (see section 3 below).*

What is iPlato's internal 'Data Protection Policy'?

The iPlato Data Security & Protection Strategy sets out the internal procedures that are to be followed by us when dealing with personal data (whether as part of iPlato Connect or the myGP App*). The procedures are followed at all times by iPlato, its employees, agents, contractors, or other parties working on behalf of iPlato.*

The Strategy is maintained centrally and submitted as part of our accreditation for the NHS Data Security and Protection Toolkit.

Where is personal data processed by iPlato stored?

All personal data processed by the iPlato platform or myGP products is stored in the UK.

How long is personal data stored for?

With respect to iPlato Connect, personal data is stored until such time as the relevant healthcare organisation ceases to be an iPlato Connect customer/user. Patient data will be deleted or anonymised within 30 days of the end of the contractual relationship.

With respect to the myGP App, personal data is stored as long as the patient remains a registered user. Once a patient de-registers and uninstalls the App all data within the App is deleted immediately.

Additionally, as required under the UK General Data Protection Regulation (UK GDPR), iPlato will comply with any legitimate requests for erasure of Personal Data from data subjects (the so called 'right to be forgotten); there is a direct deletion option available within the App. Operational data regarding the App that is maintained centrally will be stored in accordance with the company data retention policy. More information on the UK GDPR is set out below.

What data erasure methodology is employed?

Where Patient data is identifiable and separable then it is deleted in accordance with the overwrite protocol; data is deleted and then overwritten. Where data is inseparable (eg component of log files) then identifiable components are anonymised where possible.

Data in log and backup files are rotated off and overwritten. Deleted data is not recoverable in any form

What security and confidentiality arrangements are in place to protect patient data?

iPlato seeks to demonstrate its conformity with the concepts of Security & Confidentially through the following mechanisms:

1. *Implement and maintain appropriate internal policies, procedures, management systems, and processes.*
2. *Implement and maintain appropriate technical standards and features within all deployed software products and internal technical systems.*
3. *Conform to all appropriate legislation and maintain appropriate documentation and registrations.*

Policies, Management Systems and Processes

Examples of how iPlato have implemented comprehensive policies for the management of confidential information with required strategies and/or improvement plans include:

- *Appointment of a Data Protection Officer.*
- *Maintaining an Information Asset Register.*
- *Maintaining Article 30 (UK GDPR) documentation.*
- *Inclusion of key concepts into employment contracts and contractual arrangement with suppliers.*

Technical

- *Please see the iPlato System Architecture document for detailed description of all technical approaches to security including both encryption and deployment within the HSCN. This can be provided separately upon request.*

Legislation

The UK General Data Protection Regulation (UK GDPR), as tailored by the Data Protection Act (DPA) 2018, regulates the processing of personal data, held manually and on computer. The legislation applies to personal information generally, not just to health records. iPlato complies with all principles of the legislation including specifically the requirements that advocate fairness and openness in the processing of personal data and respect for data subject rights.

Does iPlato have any accreditations?

As an NHS Business Partner, iPlato completes the NHS Data Security & Protection Toolkit annually. This is a mandatory requirement to support a direct connection to the NHS HSCN network. Registration details as follows: NNG01

iPlato services are available through the UK Government Digital Marketplace on the GCloud 14 Framework.

iPlato is audited annually to maintain ISO:27001, ISO:9001 and Cyber Essentials+ certifications.

What compliance standards does iPlato meet?

UK data protection rules and codes of practice including the National Data Guardians Standards, and the guidelines imposed by NHS England and client Trust Caldicott Guardians.

What are the key impacts of GDPR on iPlato services?

The General Data Protection Regulation (EU) 2016/679 (GDPR), as defined and applied through the UK Data Protection Act 2018, has now been in force for some time.

A summary of the key impacts is provided below.

- *Mandatory requirements imposed on Controllers and Processors - iPlato maintains the required Article 30 documentation, has updated contractual documentation and adopted/modified applicable operational processes to cover requirements.*
- *Additional information to be provided to patients who use the service on the processing of their personal data - iPlato has enhanced all relevant documentation including Privacy Statement, Terms of Service and standard data sharing agreements.*
- *Patient Rights - Patient rights are communicated to patients through the iPlato privacy policy. iPlato has put processes in place to ensure required data can be ported or deleted where applicable, on the right being exercised by a patient, either directly with iPlato or through the applicable controller.*
- *Security measures and data security breach notification - iPlato security measures remain fit for purpose, with the three cornerstones confidentiality, integrity and availability. Processes and training are in place to ensure iPlato can identify and report a data breach within the required timeframe.*

Does iPlato have a registration with the Information Commissioner's Office?

Yes. Our registration reference number is ***ZA074488.***

Section 2- iPlato Connect and Toolbar

What is iPlato Connect?

iPlato Connect and associated modules (including the Toolbar) is a cloud-based middleware platform securely hosted within the HSCN and integrated directly with NHS approved clinical systems. It has a variety of functionalities/features that include secure data messages, user Toolbar, patient questionnaires, video messaging, self-book, patient triage, friends and family tests.

Who is the Controller and who is the Processor?

GPs / healthcare organisations remain the controllers. iPlato is a processor and simply processes the personal data of patients in order to provide the service to the controller.

Who "owns" the data?

Healthcare organisations, as the Controllers, 'own' all data that originates with them. Patients, as data subjects, have rights in respect of their Personal Data and Healthcare organisations have certain responsibilities in relation to such Personal Data.

What contractual commitments does iPlato make in relation to the handling of personal data?

We have prepared and contractually commit to a data processing agreement that incorporates all the requirements of data protection legislation including any requirements specified under Article 28 of the UK General Data Protection Regulation.

Do Healthcare organisations need a Data Processing Agreement with iPlato to launch iPlato Connect?

Yes, this is a key requirement under the UK General Data Protection Regulation. We include a straightforward Data Processing Agreement in our standard customer agreement documentation. Healthcare organisations are required to commit to all terms of the customer agreement (including data processing) before launching iPlato Connect.

Is patient consent required for Healthcare organisations to 'share' patient data with iPlato to launch iPlato Connect and any of its included modules such as the Toolbar?

The issue of 'Patient Consent' to data sharing is a legal issue that affects all Healthcare organisations in their capacity as Controllers of Patient data.

The data that iPlato Connect extracts from the clinical system is demographic by nature and does not include 'sensitive' or 'special category' data. However, messaging undertaken by Connect users may contain such data. Consequently, there is a higher bar to be met regarding the 1st Principle of the UK GDPR (Article 5(1)(a)). Therefore, in addition to identifying an appropriate legal basis from Article 6, Controllers need to meet at least 1 (One) processing condition from Article 9. The legislation prescribes a number of 'potential' conditions that can be relied upon - explicit patient consent is one but another and more relevant condition relates to 'health purposes', and remember Controllers only need to satisfy ONE condition.

- *Article 9 (2) (h): processing is necessary for the purposes of preventive 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…*

The legislation therefore is quite clear and patient consent is NOT required for a Healthcare organisation to 'share' sensitive patient data with iPlato because Controllers can rely on the health purposes condition.

What about informing patients?

It is the Healthcare organisation's responsibility to provide privacy information to their patients. During the launch process, iPlato provides posters and appointment cards that support Healthcare organisations to inform their patients of the services available.

What Personal Data of patients will iPlato Connect access?

iPlato Connect requires and has access to the full patient record as exists within the clinical system. This includes patient demographic information, the patient medical record as well as all appointment information regarding the specific Healthcare organisation.

How will this Personal Data be used and who will it be shared with?

Different components of the patient record are used to provide different features of iPlato Connect. The Personal Data is NOT shared with anyone unless explicit consent is received from the Patient.

Do Healthcare organisations and/or Commissioner organisations (eg: ICB's) need to carry out a Data Protection Impact Assessment before using iPlato Connect?

Yes, the UK GDPR does require the completion of a Data Protection Impact Assessment for various specific processing activity, including where processing of special category data is undertaken on a large scale or where new technologies are implemented.

However, we have significant experience helping with these assessments and can assist organisations with completing their template documentation.

To assist with the preparation of a Data Protection Impact Assessment, the Appendix contains a summary of typical template Questions and Answers that are relevant to the iPlato platform. It should be noted that the template questions and answers are typically slanted towards the impacts on GPs / healthcare organisations who use the iPlato platform and act as controllers however, some of the information is relevant to ICB's as well. ***Note: these are provided as a guide only, the preparation of the actual DPIA remains the responsibility of the Data Controller.***

Patient Communication Preferences: Can Healthcare organisations send messages (SMS & data) to patients?

YES, subject to any relevant communication preferences that may be submitted by the patient to the Healthcare organisation (see below) it is completely fine for Healthcare organisations to send messages to patients.

1. *The use of SMS / data messages is 'common place', that is there is widespread adoption across society and in Healthcare generally.*
2. *We consider that messages sent to patients by Healthcare organisations relate to direct care / the delivery of a public task. They are never marketing messages and therefore the requirements of the Privacy and Electronic Communications Regulations on consent for contact do not apply.*

What about patients who do not wish to receive messages?

Regarding patient choice of communication method: Healthcare organisations use many communication channels for patient interactions; phone calls, letters, emails, text messages, video calls etc. and collect/record both the communication details (address, number, email etc) as well as the communication preferences of individual patients. In our experience, it is quite a rare occurrence to come across a Healthcare organisation that does not have operational processes for collecting and/or modifying patient communication details and preferences.

We deal with the matter of patient communication preference as follows:

1. *During service launch we modify the launch process to take account of any recorded patient preferences that a Healthcare organisation may have pertaining to individual patients.*
2. *During service operation iPlato Connect has functionality to include/exclude patients who withdraw or modify their communication preference re SMS messaging.*
3. *On those 'rare' occasions we come across a Healthcare organisation who does not operate systems/processes to record and manage patient communication preferences, we always recommend the adoption of such processes and provide general guidance on the topic.*

Updating Patient Records

All healthcare organisations using the iPlato Connect system receive regular automated reports of 'Expired' and 'Failed' numbers which allows them to update their patient records in a timely fashion. Healthcare organisations should ensure that regular processes are in place to collect, update and maintain patient contact details, particularly mobile numbers.

Can patients opt out of iPlato Connect messages?

Yes. iPlato Connect has functionality to support patient opt-out.

Any patient requests to 'Opt-out' of SMS contact should be actioned immediately in the iPlato Connect platform.

What about bulk messaging patients to manage campaigns / Friends & Family Test?

iPlato Connect provides functionality to support the bulk messaging of patients. Individual Healthcare organisations define the nature / content of the message and identify the target cohort, then use the iPlato Connect platform to send the message; responses are automatically read-coded back to the clinical system as relevant.

It is the responsibility of individual Healthcare organisations to define the legal basis for their processing and ensure this is covered by their Privacy Notice.

On-going Promotion of Service

After service launch, Healthcare organisations should ensure a pro-active approach to advertise the existence and benefits of the service to patients. Patient awareness is a valuable tool in ensuring rapid uptake of the service. It also provides patients with the on-going choice to 'Opt-out' of the service at any time.

The following are all practical examples of different methods of publicising the service by the Healthcare organisation.

- *Waiting room posters (available from iPlato Connect).*

- *Information on website.*

- *Notification messages on general and specific correspondence i.e. prescriptions and general letters to patients.*

- *Communication with various patient groups and organisations e.g. local LINK and PPG groups.*

Section 3 – myGP App

What is the myGP App?

myGP is an App developed by iPlato for the exclusive use of patients. It is provided free of charge and distributed directly to patients by iPlato through the Android and Apple App stores. The App is integrated directly to the patient's medical records (via iPlato Connect and also via NHS supplied API's). Additionally, the App contains features that collect and process patient generated data.

The myGP App is not a GP Practice nor a Pharmacy and does not offer medical advice. myGP facilitates important patient interactions with Healthcare organisations. This includes appointment booking and cancellations as well as generic messaging functionality. In addition, the myGP App includes helpful tools to generate timely medication reminders as well as tools to assist patients in monitoring their personal health goals.

While certain information controlled, generated by, displayed within or stored in the myGP App may be helpful in providing warning of certain medical or health conditions or circumstances, the App is not designed, nor may it be used as a device to detect, diagnose, treat or monitor any medical or health condition or to establish the existence or absence of any medical or health condition. The App is not monitored by medical Practitioners or other medical professionals.

Is iPlato a processor or a controller with respect to the myGP App?

As regards the myGP App, iPlato is a processor in respect of Personal Data that originates from a Healthcare organisation's clinical system and a controller in respect of patient derived Personal Data collected and/or processed by the App.

What data of patients will the myGP App access?

myGP requires and has access to the full patient record as exists within the clinical system. This includes patient demographic information, the patient medical record as well as all appointment information regarding the specific Healthcare organisation. We call this information [GP Data].

Is patient consent required for Healthcare organisations to 'share' patient data with iPlato to enable the myGP App?

The data that iPlato Connect extracts from the clinical system is 'sensitive' or 'special category' in nature. Consequently, there is a higher bar to be met regarding the 1st Principle of the UK GDPR (Article 5(1)(a)). Therefore, in addition to identifying an appropriate legal basis from Article 6, Data Controllers need to meet at least 1 (One) processing condition from Article 9. The legislation prescribes a number of 'potential' conditions that can be relied upon - explicit patient consent is one but another and more relevant relates to 'health purposes', and remember Controllers only need to satisfy ONE condition.

- *Article 9 (2) (h): processing is necessary for the purposes of preventive 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…*

The legislation therefore is quite clear and patient consent is NOT required for a Healthcare organisation to 'share' sensitive patient data with iPlato, because Controllers can rely on the health purposes condition.

Will the myGP App collect any other data?

Yes. Some registered users of the myGP App may choose to input information into the App for example when they fill in forms in the App, use certain App Cards or send us direct communications; they provide their consent for us to process this information.

We may also collect certain data about users' use of the myGP App such as:

i. *technical information, including type of mobile device used, a unique device identifier, mobile network information, mobile operating system, and time zone setting;*

ii. *information either accessed through the user device or stored on the device which the user has explicitly consented to sharing, and the providence of that data including the device used to collect that data, time, date; and*

iii. *details of the use of the myGP App.*

Not all of this data is Personal Data. We use it to better understand the use of the services and make improvements.

Collectively we call all of this data [myGP Data].

Who "owns" the data?

Healthcare organisations 'own' their Patient Data [GP Data] and iPlato 'owns' App specific data [myGP Data].

Where is the data stored?

All data relating to Patients is held on UK hosted availability zones of the AWS cloud and transferred via HSCN).

How long is the data stored for?

All, being both GP Data and myGP Data is stored as long as the Patient remains a registered App user. Once a Patient de-registers all data is deleted or anonymised.

Additionally, under the UK General Data Protection Regulation (UK GDPR), iPlato will comply with any legitimate requests for erasure of Personal Data from data subjects (the so called 'right to be forgotten'); there is a direct deletion option available within the App.

Will myGP Data be shared with Healthcare organisations and or other 3rd parties and if so, is Patient consent required?

myGP Data will never be sold to anyone and will only ever be shared with 3rd parties including the patient's GP with the explicit consent of the respective Patient.

There are very limited exceptions to the above rule. Full details are contained within the App Privacy Policy however in summary the only exceptions are:

i. *If we are under a duty to disclose or share personal data to comply with any legal or regulatory obligation; or*

ii. *To enforce or apply our Terms and other agreements or to investigate potential breaches of such Terms; or*

iii. *To protect the rights, property or safety of iPlato, our customers, or others.*

What is the myGP App's privacy policy?

Please see the myGP 'App Privacy Policy' which can be viewed here: App Privacy Policy - myGP

Can Healthcare organisations control the use of the myGP App by patients?

myGP is an App developed for the exclusive use of Patients. It is provided free of charge and distributed directly to Patients by iPlato through the Android and Apple App stores. The myGP App is provided for and available to all UK registered Patients. GP's, ICB's or other NHS bodies have no capacity to influence, restrict or control access to the App for any Patient.

Can patients 'Opt-out' of the myGP App?

Yes, Patients can cease using and/or uninstall the App at any time.

APPENDIX – SAMPLE DPIA QUESTIONS AND ANSWERS

General Overview

What are the main aims of the iPlato platform?	*To communicate electronically with patients using various digital tools eg SMS, data messaging, video, etc.*
List the main activities of the project.	*Determined by the modules procured. Example core functionality of the main modules includes;* ▪ *To send appointment reminders, allow patients to cancel appts via text and App and provide reminders for clinical campaigns.* ▪ *To initiate and participate in chat and/or video sessions with a patient.* ▪ *To undertake service signposting to Patients.* ▪ *To collect and process information from patients including survey responses, health and other relevant data.*
What are the intended outcomes?	*Convenient, immediate, secure and effective method of communication with patients. To collect relevant information from patients and signpost relevant services to patients.*

Data

Who are the Data Subjects? i.e. the people whose data will be held	*Registered patients.*
What Data Classes will be held on this system (ie the actual data fields)?	*Demographic data provided via Partner API to include: Name, DOB, Address, Postcode, Email address, Mobile Number, NHS Number, Gender, Appointment Details, SMS consent.*
Will this system/process include data which was not previously collected?	*No*
Does the system/process include new or amended identity authentication requirements that may be intrusive?	*No*
What checks have been made regarding the adequacy relevance and necessity of data used?	*The data used is input by the Patients directly or accessed via the GP Clinical System which provides specific demographic data fields. All unnecessary fields are discarded and only required fields are retained.*

Can the system/process use pseudonyms or work on anonymous data?	*No, patients must remain identifiable to manage messaging.*
Can the data subjects opt out of their data being added to the system/used by the process, and if so is this publicised?	*Yes, patients can opt out of being contacted via video, SMS or data message. The iPlato system has appropriate consent management functionality.*
Who are the partners for the data sharing?	*[Name of Healthcare organisation]* *iPlato Healthcare Ltd*

Data Security

Who will use the system/process and have access to the data?	*System access at iPlato is restricted to iPlato employees who require it to perform their role.*
What training have users had in patient confidentiality?	*All iPlato employees undertake annual NHS approved e-learning via eLfH. In addition, they receive a verbal Data Protection briefing on induction and Data Protection e-bulletins as relevant.*
Will the data be shared with any third party organisations?	*No – the only sharing is with established processors who provide messaging / video functionality*
Where will data be held?	*All data is held in UK hosted availability zones of the AWS cloud and transferred via the HSCN network*
What format will data be stored in?	*Binary data*
Does the system/process change the way data is stored?	*No*
How will staff access and amend data?	*Access to patient data is restricted to key staff. Access is over VPN and MFA is required.* *It's not possible for staff to amend data using our system.*
How will data be transferred from/to clinical system?	*Via approved NHS / clinical system API*
Are you transferring any personal and/or sensitive data to a country outside the European Economic Area (EEA)?	*No*

What security measures have been taken to protect the data?	*Encryption: backups within S3; VPN encryption; SSL encryption between endpoints; syncing with clinical systems done on HSCN (formerly N3 network) data at rest on multiple Amazon cloud instances.* *Access control: 3 levels of access exist; validity duration; minimum password length; required characters; lockout; forced change password; no repeat password; hashing mechanism SHA256.* *Archived data is minimised and pseudonymised: deleting names, phone numbers, email addresses, address (retain postcode, patient ID, NHS number).*
Is there a useable audit trail in place for the asset?	*Full logging for write/update features.*
How often will the system/process be audited?	*Annually*
Who supplies the system/process?	*iPlato Healthcare Ltd supplies the system.*
Is the supplier of the system/recipient of the data registered with the ICO? Please give the registration number.	*iPlato Healthcare Ltd is registered with the ICO.* *ICO Registration: ZA074488*
Has the organisation completed the DSP toolkit?	*Yes – see Organisation Search (dsptoolkit.nhs.uk)* *– Ref NNG01*
What business continuity plans are in place in the case of data loss/damage as a result of human error/ computer virus/ network failure/ theft/ fire/ flood / other disaster?	*iPlato has appropriate business continuity arrangements in place to ensure that systems / data can be restored as required.*

Data Quality

Who provides the information for the asset?	*All patient data resides in the Clinical Management System. The Healthcare organisation provides the data to the iPlato system via the approved and assured Partner API's and/or NHS centrally approved and maintained IM1 API interfaces*
Who inputs the data into the system?	*The Controller ie: the Healthcare organisation in the normal course of operations. All subsequent transfers to the iPlato system are automated.*

How will the information be kept up to date and checked for accuracy and completeness?	*Data in the iPlato system is refreshed periodically via the Partner API – this is an automated process.*
Can an individual (or a court) request amendments or deletion of data from the system?	*Yes*

Ongoing Use of Data

Will the data be used to send direct marketing messages?	*No*
Does the system/process change the medium for disclosure of publicly available information?	*No*
Will the system/process make data more readily accessible than before?	*Yes, patients will have easier access to appointment bookings and be able to view their medical record if the Healthcare organisation uses a compatible clinical system.*
What is the data retention period for this data?	*Patient data will be retained for the duration of the contract and will be securely deleted by iPlato within 30 days of contract end.*
How will the data be destroyed when it is no longer required?	*Data is overwritten and then deleted. Data in log and backup files are rotated off and overwritten. Deleted data is not recoverable in any form*

Risk Analysis

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**myGP Product**	**Likelihood of harm**	**Severity of harm**	**Overall risk**
Illegitimate access to data resulting in data breach / patient distress / reputational damage				
RISK: Healthcare organisation / commissioning body communicates with wrong patient *MITIGATIONS:* • *Healthcare organisation staff provided with training on iPlato platform* • *Name and NHS number displayed in Connect to support identification* • *Toolbar requires sender to confirm corresponding with correct patient before sending*	Connect	Remote	SEVERE	Medium
RISK: Shared Patient device use *MITIGATIONS:* • *myGP App requires passcode / device biometrics* • *Messaging is generic in nature*	All	Remote	SEVERE	Medium
RISK: Lost/stolen Patient device *MITIGATION: App access requires passcode / device biometrics*	All	Remote	SEVERE	Medium
RISK: Patient actively shares comms / medical info with another party *MITIGATION: n/a - Patient responsibility*	All	Possible	Minimal	Low
RISK: Toolbar download URL copied and shared with unauthorised recipient *MITIGATION: DOB and mobile number must be entered to access download URL - 3 attempts and then download link rendered unusable*	Toolbar	Remote	SEVERE	Medium

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**myGP Product**	**Likelihood of harm**	**Severity of harm**	**Overall risk**
RISK: Report from Connect forwarded to incorrect recipient *MITIGATIONS:* • *Minimal personal data included in reports, if any* • *iPlato staff training / SOPs ensure staff understand need to exercise care*	Connect	Remote	Significant	Low
RISK: Unauthorised access at Healthcare organisation or iPlato (eg: computer left unlocked) *MITIGATION: iPlato has secure working practices (eg: auto-locking of screens) and staff training and awareness* *ASSUMPTION: Healthcare organisation has similar secure working practices, staff training and awareness*	Connect (at practice) All (at iPlato)	Remote	Significant	Low
RISK: Unauthorised access by Healthcare organisation staff / IT provider or authorised access by Healthcare organisation / IT provider that is misused *MITIGATION: Healthcare organisation staff provided with training on iPlato platform* *ASSUMPTIONS:* • *IT provider contract includes confidentiality clauses* • *Healthcare organisation/ IT provider have disciplinary measures in place*	Connect	Remote	SEVERE	Medium
RISK: Unauthorised access to data by myGP employee / authorised access that is misused *MITIGATIONS:* • *myGP system access is controlled by role based permissions.*	All	Remote	Significant	Low

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**myGP Product**	**Likelihood of harm**	**Severity of harm**	**Overall risk**
• *Employee training and guidance is provided, and disciplinary process is well established*				
RISK: Brute force attack *MITIGATION: myGP has robust system security and effective and tested backup and restore capability – CE+ certification*	All	Remote	SEVERE	Medium
RISK: Malware *MITIGATION: Appropriate security guards against malware – CE+ certified*	All	Remote	SEVERE	Low
RISK: Deployment error makes data vulnerable *MITIGATION: Deployment support / guidance guards against deployment errors*	All	Remote	SEVERE	Medium
RISK: Vulnerability in operating system *MITIGATION: Significant testing and ongoing maintenance guards against vulnerabilities*	All	Remote	SEVERE	Medium
Unwanted changes to data resulting in data breach / patient distress / reputational damage				
RISK: Inaccurate data in clinical system due to Healthcare organisation error *ASSUMPTION: Healthcare organisation staff training and data quality procedures are in place*	All	Remote	SEVERE	Medium
RISK: Inaccurate data displayed / shared / written to clinical record due to iPlato platform processing error *MITIGATION: End-to-end feature testing is undertaken / monitoring & reporting*	All	Remote	SEVERE	Medium

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**myGP Product**	**Likelihood of harm**	**Severity of harm**	**Overall risk**
RISK: Personal data written back to clinical record without Healthcare organisation oversight *MITIGATION: Healthcare organisations decide whether to apply coding to specific messaging.* *Patient responses are sent to iPlato Connect inbox - Healthcare organisation responsibility to correct patient record if required*	Connect	Remote	Significant	Low
RISK: Assigning incorrect code causes error written to patient record *MITIGATION: Healthcare organisations specify codes to be used and iPlato staff training / awareness ensures staff understand the need to exercise care* *ASSUMPTION: Healthcare organisation staff training is in place*	Connect	Remote	SEVERE	Medium
RISK: Unauthorised access to Healthcare organisation results in changes to configuration / written info or sends messages *MITIGATIONS:* • *Auto log-out* • *Different levels of account access at Healthcare organisation* *ASSUMPTION: Healthcare organisation security is at an appropriate level*	Connect	Remote	SEVERE	Medium
RISK: Inappropriate changes made by iPlato employee *MITIGATIONS:* • *iPlato platform access is controlled by role-based permissions* • *System / server access is audited* • *Employee training and guidance is provided, and disciplinary process is well established*	All	Remote	SEVERE	Medium

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**myGP Product**	**Likelihood of harm**	**Severity of harm**	**Overall risk**
RISK: Brute force attack *MITIGATION: iPlato has robust system security and tested backup and restore capability – CE+ certification*	All	Remote	Significant	Low
RISK: Software development change leads to integrity issues *MITIGATIONS:* • *Change management and ability to roll-back* • *Frequent refresh of data via API will address any integrity issues*	All	Remote	Minimal	Low
RISK: Hardware failure causing data corruption *MITIGATIONS:* • *Hardware security & maintenance arrangements guard against failure* • *Backup arrangements and frequent refresh enable effective data restore*	All	Remote	Minimal	Low
RISK: API or comms provider error leads to data changes *MITIGATIONS:* • *Use of APIs and comms providers well established* • *Any identified errors are actively managed (and reported as required)*	All	Remote	Minimal	Low
Disappearance of data resulting in data breach / loss of service / patient distress / reputational damage				
RISK: Inability to provide services (eg: appointment bookings / repeat prescription / medical record access) due to Healthcare organisation not enabling these features *MITIGATIONS:* • *Patients are referred to the Healthcare organisation to query directly* • *Healthcare organisation staff training and procedures are provided*	myGP App Connect	Possible	Significant	Medium

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**myGP Product**	**Likelihood of harm**	**Severity of harm**	**Overall risk**
RISK: Unauthorised deletion by iPlato employee *MITIGATIONS:* • *iPlato employee training and guidance provided, and disciplinary process well established.* • *Backup arrangements and frequent refresh enable effective data restore*	All	Remote	Significant	Low
RISK: App / platform downtime *MITIGATION: Downtime is handled as a priority and iPlato has effective and tested backup and restore capability.*	All	Possible	Significant	Medium
RISK: Brute Force (eg: Ransomware) attack *MITIGATION: iPlato has robust system security and tested backup and restore capability – CE+ certification*	All	Remote	Significant	Low
RISK: Hardware failure causing data loss *MITIGATIONS:* • *Hardware security & maintenance arrangements guard against failure.* • *Backup arrangements and frequent refresh enable effective data restore*	All	Remote	Minimal	Low
RISK: Software failure causing data loss *MITIGATION: Change management processes are established, and backup arrangements enable effective software restore*	All	Remote	Minimal	Low
RISK: Physical theft *MITIGATION: Appropriate physical security guards against theft and effective access controls guard against access if stolen*	All	Remote	Minimal	Low

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**myGP Product**	**Likelihood of harm**	**Severity of harm**	**Overall risk**
RISK: Comms provider fails to deliver messages *MITIGATION: Delivery receipts received, and ongoing use of comms provider has not caused any serious issues*	All	Remote	Significant	Low
RISK: Attachments fail *MITIGATION: Tried and tested functionality*	Connect (Toolbar)	Remote	Minimal	Low

NOTE: iPlato has undertaken a robust exercise to identify and mitigate risk, however we cannot guarantee that the above list is exhaustive.