Data Privacy Impact Assessment

askmyGP System

Document Contents

Document Control

Status	Version	Author	Change Description	Date
First draft	0.01	Adrian Stavert-Dobson	N/A	21/05/2018
Approved	1.00	Adrian Stavert-Dobson	Finalised	12/07/2018

Approved	1.01	Adrian Stavert-Dobson	Updated and approved	12/11/2018
Revised	1.02	Phil Walker	Updated	4/12/2019
Revised	1.03	Phil Walker	Updated	14/01/2020

Document Owner	Harry Longman
Version Control	1.01
Document Date	12/11/2019
Document Approval	IG Forum
Document Classification	Public
Document Distribution	Intranet
Document Review date	14/01/2021
Document Name	IG0040 Data Privacy Impact Assessment

1.   Introduction

The General Data Protection Regulation requires that a Data Privacy Impact Assessment is carried out on systems which contain confidential data in higher risk categories. This document fulfils that requirement.

2.   Purpose

This document represents the Data Privacy Impact Assessment for Version 3 of the askmyGP product.

3   Scope

This policy applies to the askmyGP system.

4   Applicability

This policy is relevant for IT staff of GP Access Ltd, the GP Access Ltd partners and customers of GP Access Ltd.

The need for a DPIA

The askmyGP system facilitates a patient's electronic communication with their GP Practice. The patient can enter a query or specify their clinical symptoms which are then routed to Practice staff to action accordingly. The patient's name, gender, date of birth and symptomatology are captured, stored and retrieved by healthcare professionals. In addition, the patient may enter into an asynchronous dialog with a clinician or administrator and disclose further health information. This data is also stored in the application database.

Accidental or deliberate disclosure of the data to parties beyond the GP Practice and clinicians involved in the patient's care could contravene the individual's right to privacy.

The General Data Protection Regulation requires that a DPIA is carried out in circumstances where processing is "likely to result in high risk". Article 35(3) provides some examples when a processing operation could be considered high risk – this includes 'special categories' of data. Special categories include health data.

Whilst the askmyGP system does not process data on a large scale, on balance it was felt that a DPIA should be constructed for the service. The askmyGP system executes several processing operations, however these operations constitute a similar level of risk. As such, this DPIA covers all askmyGP processing operations.

Processing of the data

Purpose of processing

Data is captured and processed for the purpose of facilitating patients gaining access to primary care services. The information is used by the patient's Practice to establish the optimal means by which care can be provided. To inform this decision-making, the patient is required to disclose details of their query which might be administrative in nature (e.g. I need a repeat prescription) or clinical (e.g. I am suffering from backpain). In some circumstances, the patient may choose to disclose sensitive information such as the presence of a sexually transmitted disease.

Patients benefit from the service by being able to participate in a demand-led workflow, ultimately reducing the time required to see a GP or gain access to other care services. GP practices benefit by having a more predictable and manageable flow of patients. askmyGP is a commercial venture by GP Access however the company does not benefit directly from

patient identifiable data (i.e. the data is not used for marketing products or services to individuals).

Nature of processing

Patients will typically gain access to the service from either a direct URL publicised by the Practice or from a link on the Practice website. The URL or link will contain sufficient information to uniquely identify the Practice.

Prior to entering any data, the user is presented with a privacy statement and terms of use explaining the purpose of the data and with whom it is shared. Explicit consent is required in order to gain access to the service. Data processing then takes place on the basis of this consent.

Data is captured into an electronic web-based form which the user accesses via one of the supported browsers. The user is required to identify themselves by their name, gender and date of birth. In the future, the data may be supplemented by the patient's NHS number. The user may enter the details not for themselves but for someone for whom they are caring.

The data is only disclosed to the Practice with whom the patient is intending to access care services. Individual Practices are responsible for ensuring that only appropriate personnel are exposed to the clinical data as would typically be set out in their local information governance policy.

The technology employed uses simple web-services linked to a secure MySQL database. The practice-facing component is hosted in an HSCN environment and is therefore subject to the security features of that network. Hosting is provided by an established and experienced third party called Xicon Limited. All data is retained in the UK.

Information retention and deletion

The data will be stored in an identifiable form for a period of 2 years. in line with the NHS Records Management Code of Practice. Two years after the date of the first database transaction, a yearly scheduled cleanse of the database will be undertaken. An SQL script will be used to remove legacy data older than 2 years without breaking referential integrity.

After the 2 year retention period, the data may be retained in an anonymised form for statistical purposes.

On decommissioning of the system, GP Access will notify its hosting partners and trigger their irretrievable data destruction processes.

Should an individual patient request their personal data to be deleted, this process can be conducted by the practice staff using dedicated functionality. In addition, GP Access could undertake this task if required.

Subject access request

The GP Access Subject Access Request Procedure is set out at IG0042 Subject Access Request Procedure.

Scope of data

The following identifiable information is captured:

- First name and surname

- Date of birth

- Gender

- Ideas, concerns and expectations with regards to the patient's query or symptomatology *

- Time and date of the query

- Content of the messaging dialog with administrative or clinical practice staff *

- Telephone number

- Email address

- NHS Number added by practice staff

Data items marked * could be considered to represent 'special categories' of data as they directly relate to health information.

The number of requests submitted by patients to each practice varies significantly between practices. However, 100 requests per day might be typical.

The service is not intended to be used by children. Parents may raise requests with regards to their children, but these would be attributed with the parent's identity. The first name, surname, date of birth and gender of the child is maintained.

Sharing with third parties

GP Access Ltd may share the data with trusted third parties with whom the company has a data sharing agreement in place. However, the data will be transformed, prior to its transmission, in such a way that it is truly anonymised. This will occur in two phases:

1. Separation of the identifiable data and non-identifiable data followed by replacement of the identifying foreign key with a new key. The resulting anonymised data would be difficult or impossible to be repatriated with the identifiable dataset and would be impossible for a recipient of the anonymised data alone to establish identity.

2. A human review of all free-text fields in the dataset to ensure that no identifiable data had been entered by the user into these fields. Any such information would be deleted prior to transmission.

The use of data for these purposes are included in the privacy statement presented to the user on initial sign-up and form part of the consent process.

Necessity and proportionality

The necessity for the processing of personal data is set out for users in the Privacy Notice at https://askmygp.uk/askmygp-application-privacy-policy/.

Data is processed with the user's consent which is gained prior to accessing the service. Data is processed because the user has consented to the use or because it is in the company's legitimate interests. In order for clinicians to provide accurate clinical advice, it is necessary to uniquely identify the patient such that other local clinical systems can be consulted to understand the patient's history. Thus, without capturing patient identifiable data and the associated symptomatology, it would not be possible to provide the service or deliver care safely. Should users choose not to share their data, patients can still gain access to their practice using the telephone or walk-in.

The system functionality and data capture scope are subject to change control processes (see IG0030 Managing Change Which Involves Personal Data). Each item of new functionality is reviewed in GP Access's JIRA environment. Any changes to the product are reviewed to determine whether there is a material impact on the Data Privacy Impact Assessment and the document is updated accordingly. Should new personal data fields be captured, they would only be accepted into the development process if it could be demonstrated that the data was within the scope of the Privacy Notice and was required for the safe and efficient delivery of the service.

Risk assessment

Scope

Patient identifiable data is held only on the database server and is accessible to the application server. Both components are hosted in the cloud by a reputable hosting provider. As such, this risk assessment does not include factors related to the personal computing assets of employees and contractors who do not have access to the server components. These assets are architecturally discrete and pose sufficiently low risk to not warrant further examination.

Privacy and security hazard log

Privacy/Security hazard	Controls	Likelihood of harm	Severity of harm	Overall risk
Intruder exploits operating system vulnerability on application server or database	Server is accessible only by VPN over SSH. The Ubuntu server is set to patch automatically Weekly checks undertaken to ensure all relevant server components are up to date. Database and application server default passwords have been changed. All passwords are strong. Only the required packages are installed on the server to ensure no extraneous services are running. Fortinet firewalls at each endpoint. VLAN enabled per customer environment. VDOM enabled. Xicon have intrusion detection system in place. Database content is encrypted. The application server and database have been included in the system penetration testing.	Remote	Significant	Low ALARP

A user who is not authorised to access the application or database server gains access	Access to the live servers is limited to only two individuals.	Possible	Significant	Medium
	Access is controlled according to the Company's User Account Authorisation Policy (IG0018) and logged in IG0036 Application Access Authorisation Log.			ALARP
	Access to the servers is revoked when staff leave the organisation as set out in User Account Authorisation Policy (IG0018).			
	The server does not have a GUI so it is not susceptible to phishing or instant messaging threats.			
	Database content is encrypted.			
	Access to the servers can only be gained by VPN over SSH.			
	Servers are protected by strong passwords			
	Accounts are specific to individual users.			
	Web server is protected behind NetScaler, only https access is available to NetScaler.			
	All access to the servers is recorded in the Apache log and Authentications logs including failed login attempts.			

Application or database server is subject to malware attack.	Server is protected by ClamAV Anti-Virus software. Daily anti-virus scans are undertaken. Servers are based on Ubuntu which is unlikely to be subjected to malware attack. Server is set to automatically patch in order to address any potential security flaws. Weekly checks undertaken to ensure all relevant server components are up to date. Server does not have a GUI so is less susceptible to attack. Users unable to navigate to suspicious website, etc. Access to server and the services installed on the server are carefully controlled. Fortinet firewalls at each endpoint. VLAN enabled per customer environment. VDOM enabled Periodic vulnerability scans are undertaken by Xicon. As the server is hosted remotely, users are unable to insert usb drives or other peripherals into the infrastructure. Xicon has policies and procedures in place to minimise risk of malware attack.	Remote	Significant	Low ALARP
Security threat introduced by client workstation connecting into the database or application servers.	Access to the servers is limited to just two members or staff using two workstations. The connectivity framework employed means that the local workstation and server components remain architecturally discrete. File transfer is controlled and limited to ftp. Client workstations have up to date antivirus software installed. Client workstations are subject to IG and remote working policy.	Remote	Significant	Low ALARP

Disclosure of confidential data due to theft of workstation or portable device.	By policy, patient identifiable data is not stored on local workstations or portable devices and to do so would be subject to disciplinary measures. Use of remote working is subject to the company policy IG0007 Mobile Computing and Teleworking Policy and Guidelines. All data in the database is encrypted.	Remote	Significant	Low ALARP
Disclosure of confidential information due to location of workstation (e.g. local on-lookers).	Patient identifiable data is encrypted in the database and cannot be viewed in human-readable form by staff. Remote working is subject to IG0007 Mobile Computing and Teleworking Policy and Guidelines.	Remote	Significant	Low ALARP
Disclosure of personal data due to vulnerabilities in the hosting organisation or data centre, (e.g. physical access).	Xicon is a reputable provider of hosting services. Whilst the precise security and policy procedures have not been made available for inspection by GP access, Xicon is compliant with ISO 27001:2013 and, consequently, it is assumed that appropriate measure are in place. Xicon are also compliant with: ISO 14001:2004 Environmental Management System Standard OHSAS 18001: 2007 Occupational Health & Safety Management System Standard ISO 50001:2011 Energy Management System Standard PCI-DSS Payment Card Industry Data Security Standard BS5979 and BS8418	Remote	Significant	Low ALARP

Data loss due to loss of application database.	The hosting infrastructure includes a second datacenter to which the application can fail over. Database is subject to regular back ups as set out in IG0039 Back Up and Restore Policy. The Company has a Business Continuity Plan (IG0027 Business Continuity Plan.) The database is managed by a reputable hosting provider and supported by professional personnel. The MySQL database employed is industry standard and staff are familiar with its configuration and operation. Loss of historical data would not significantly compromise care delivery as the details of consultations are recorded in separate local clinical systems. Servers are monitored using Xicon's N-Able monitoring system from Solarwinds.	Remote	Signifi cant	Low ALA RP
Disclosure due to improper handling of backups containing patient identifying details.	Backup is subject to a backup and restore policy. Backup files are maintained by the hosting provider and are not kept outside of this environment. All identifiable data is encrypted in the database. It is assumed that the hosting provider as appropriate measures in place to handle backup data according to ISO 27001.	Remote	Signifi cant	Low ALA RP
Disclosure due to use of stored passwords.	Use of passwords is subject to company security policy. Passwords should not be written down or stored in any other form.	Remote	Signifi cant	Low ALA RP
Confidential data is transported outside the UK	Xicon data centres are located entirely in the UK.	Remote	Signifi cant	Low ALA RP

Patient-facing application subject to malicious attack (e.g. code injection)	The application has been developed using modern coding techniques to minimise code and sql injection. The front-end application has been subject to penetration testing by an independent expert organisation. Identified vulnerabilities have been managed accordingly.	Possible	Significant	Medium ALARP
User gains access to a different user's account via the patient-facing application	Account access is governed by username and password entry. Passwords are validated by the zxcvbn password strength estimator. Through pattern matching and conservative estimation, the algorithm recognises and weighs 30,000 common passwords, common names and surnames according to US census data, popular English words from Wikipedia and US television and movies, and other common patterns like dates, repeats (aaa), sequences (abcd), keyboard patterns (qwertyuiop), and l33t speak. The details of the username and password are not cached locally. Passwords are masked on data entry by default. Malicious users would typically only be able to access the details for one patient (i.e. for the user they logged in as) but would not be able to see the confidential information of anyone else. Password reset emails are only valid for 24 hours. Account login is throttled, so that brute force logins are not possible.	Possible	Significant	Medium ALARP
User of patient-facing application sees confidential data for another patient	All patient data in the database is linked to a unique user ID which can only be accessed by the logged in user. The system has been tested to ensure that it is only possible to view data for the currently logged in user. Penetration testing has validated that this scenario cannot occur.	Remote	Significant	Low ALARP

Unauthorised user gains access to the practice-facing application	The practice-facing application is hosted on the HSCN Virtual Private Network which is only accessible to healthcare organisations. Access to the practice-facing application is controlled by user-specific usernames and passwords. The system ensures that only strong passwords can be set by users. The system requires that the password for the initial administrator account is changed on first use. The username is the email so duplicates are not possible. Passwords are obscured during creation by default.	Remote	Significant	Low ALARP
Staff at one practice is exposed to patient data at another practice	All patient requests and other patient data is logically linked to the practice with whom the patient is communicating. Users of the practice system are unable to retrieve any data not relating to their practice. Users are logically linked only to their own practice and therefore cannot access data for other practices. The system has been tested to ensure that only information relating to the relevant practice user is accessible.	Remote	Significant	Low ALARP
Data shared with a third-party accidentally contains identifiable data	Data to be shared with third-parties is extracted in an anonymised form. A meaningless identifier which cannot be linked back to the original identifying data is then attached. Identifying datasets are not shared with third-parties. These remain encrypted in the application database. Free text fields are manually reviewed by the IG Lead to ensure they do not contain data which could identify the individual user or any other individual referenced.	Remote	Significant	Low ALARP

Risk matrix

		Severity		
		Minimal	Significant	Severe
Likelihood	Probable	Medium	High	High
	Possible	Low	Medium	High
	Remote	Low	Low	Medium

Measures to reduce risk further

Pen testing is regularly conducted, and the system is constantly monitored.

Risk assessment summary

The risk assessment above has demonstrated that the privacy and security risks identified have been mitigated to As Low As Reasonably Practicable and are therefore considered to be Tolerable. However, work will continue to monitor these hazards and the associated risk in live service and as changes are made to the system.

6   Policy Review

GP Access Ltd Management will audit the policy periodically.

7   Policy Non-compliance

Employees and contractors violating this policy will be required to meet with their manager and may face disciplinary measures or termination of contract.

8   Policy Exceptions
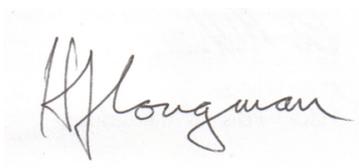
Exceptions must be approved by the GP Access Ltd IG Forum.

9   Related Policies, Procedures and Guidelines

As referenced in above material.

11   Management Approval

On behalf of GP Access Ltd

Approved By:			
Name:	*Role*	*Signature*	*Date:*
Harry Longman	Chief Executive		January 14, 2020

Date for next Review:	January 14, 2021