engage
HEALTH SYSTEMS

TITLE:

PSF Data Protection Impact Assessment

Version 10

Connected | Supported | Engaged

engagehealth.uk

PSF Data Protection Impact Assessment

Introduction

This Data Protection Impact Assessment (DPIA) records the process and methods of how sensitive data is managed in the Patient Services Framework (PSF); the underlying platform for the Engage family of products. It is based on the guidance published by the ICO (V0.3.2) and forms part of our BS EN ISO/IEC 27001:2017 Statement of Applicability.

Scope

The PSF is the collective name for the components that deliver the Engage suite of products. Whilst many elements are shared between services, the customer facing products that this DPIA covers are:

Engage Consult	On-line consultation service for primary care
Engage CRS	On-line consultation service for specialist care settings
EnCompass LT	Clinical workflow and clinical system interface service though the Engage Client
Engage Touch	Patient arrivals touch screen and questionnaire system, with support for data capture from medical devices such as scales and BP cuffs
My EHS	The customer facing portal to manage the services on the PSF

Requirement

The PSF provides an array of patient facing services and, as such, handles sensitive data. Engage Health acts as both a Processor and Controller, depending on the service delivered. For an architectural and technical overview, please refer to **DEV103 - PSF Technical Architecture** . A key feature of the services is the safe and controlled exposure of sensitive data to both medical staff and patients.

Purpose of the processing

The specific Purpose varies from service to service, but all share these aims:

- Empowering the patient
- Speeding up access to appropriate services
- Delivering efficiencies to the care providers

Subjects of the processing

The services process data for four classes of subject, all of whom are located in the UK:

- Online Patient Service (OPS) users
- An OPS user as a patient
- Patients with a proxy relationship with the OPS user
- Healthcare professionals

For the purpose of this document, "Healthcare professionals" includes health care organisations support and administrative staff as well as their clinical members.

Nature of the processing

The services involve the collection, ordering and presentation of patient data from two sources:

- Patient entered Either in the capacity of "Self" or by a duly authorised proxy.
- NHS data Most often, the patient's medical records held in their surgery clinical system

Depending on the nature of the service and the stage of the transaction, information may be presented to the OPS user or a healthcare professional. This may involve routing the message internally between authorised staff members or extending the contact by engaging in a digital 2 way conversation with the patient.

In addition to textual messaging, a surgery may choose to converse using the built-in video communication capability.

Given the nature of the processing, the risk of a breach or inadvertent disclosure must be considered at all times. External agencies are engaged to provide independent testing and evaluation of the services in accordance with industry best practice and NHS requirements.

Location of the processing

Data is processed in two locations:

Local processing Short term storage on the organisation's local device in compliance with their data handling processes. Additionally, the services locally encrypt some data which is held resident on device.

Remote processing All off-site information is processed on an assured platform that has been certified to handle clinical data. When acting as a Data Controller, information is held on the same encrypted, replicated platform storage that is again certified to process sensitive data.

Data is held in a sovereign UK facility and no data is processed outside the UK, with the exception of data presented to OPS users accessing their data via the services from overseas.

Duration of the processing

The duration of processing is dependent on the class of data:

Patient Data

As elements of the PSF deliver services under framework agreements with NHS England, there are areas of data that are governed by the rules and exemptions for Healthcare data. This includes OPS account data (including demographics and those of proxy patients) and audit/log records.

Notwithstanding this, the data belongs to the OPS user, and they are placed in control of their data. User accounts and associated information persist indefinitely unless any of the following conditions are met:

- The individual exercises their rights under GDPR to delete their account
- The data controller requests deletion (usually after end of contract)
- 10 years after patient death
- 100 years after last account activity

These data retention periods are in line with Appendix 3 of the Records Management Code of Practice for Health and Social Care (2016) published by the IG Alliance. In areas of ambiguity and system design, the principle of holding as little data for as short a period as possible will be adhered to. OPS user status can be determined automatically from national directories, such as the Spine or their registered primary care clinical system.

Where a patient engages with the services in a "Guest" capacity (i.e. does not operate under the context of an OPS account), the data is retained according to the preferences of their claimed Data Controller. The default is for deletion one month after the last activity on the encounter, but a customer can extend this up to one year.

In the event that an OPS user contacts us with a Data Subject Access Request, we follow our DSAR process (IG007 - Data Subject Access Requests) which involves informing the data controller immediately.

Staff Data

For healthcare professionals using the system, basic demographic and account data is managed. Account deletion can either be carried out by the user or their organisation's designated administrator. There is no automatic deletion and organisations are encouraged to record access granted to our services for inclusion in their staff leavers process.

Nature of Data Processed

The data processed varies for each class of data subject. Some health information is highly sensitive and so falls under "Special Category" data (GDPR Article 9).

Engage Consult

Subject	Data	Requirement	Local?	Remote?
OPS User	Full name	Mandatory	Yes	No
OPS User	Postcode	Optional	Yes	No
OPS User	Telephone number	Mandatory	Yes	No
OPS User	e-mail address	Mandatory	Yes	No
OPS User	Salted and hashed password	Mandatory	Yes	No
OPS User	NHS Login identity	Optional	Yes	No
OPS User	Audit data	Mandatory	Yes	No
Patient	Audit data	Mandatory	No	No
HCP				
HCP	Full name	Mandatory	Yes	No
HCP	Gender	Optional	Yes	No
HCP	e-mail	Mandatory	Yes	No
HCP	Linked orgs	Mandatory	Yes	No

HCP	Salted and hashed password	Mandatory	Yes	No
HCP	Message data	Mandatory	Yes	No
Patient	Full name	Mandatory	Yes	No
Patient	Gender	Mandatory	Yes	No
Patient	Date of birth	Mandatory	Yes	No
Patient	NHS number	Optional	Yes	No
Patient	Address	Optional	Yes	No
Patient	Postcode	Optional	Yes	No
Patient	Telephone number	Optional	Yes	No
Patient	e-mail address	Optional	Yes	No
Patient	Registered surgery	Mandatory	Yes	No
Patient	Patient entered medical data	Optional	Yes	No
Patient	Appointment data	Optional	Yes	No
Patient	Message data	Optional	Yes	No

Engage Touch

Subject	Data	Requirement	Local?	Remote?
Patient HCP	Audit data	Mandatory	No	No
HCP	Full name	Mandatory	No	No *
HCP	Gender	Optional	No	Yes

Patient	Full name	Mandatory	No	No *
Patient	Gender	Mandatory	No	No *
Patient	Date of birth	Mandatory	No	No *
Patient	Address	Optional	No	No *
Patient	Postcode	Optional	No	No *
Patient	Telephone number	Optional	No	No *
Patient	e-mail address	Optional	No	No *
Patient	Patient entered medical data	Optional	No	No *
Patient	Appointment data	Optional	No	No *

*Only applicable if mobile arrivals enabled

Context of the processing

OPS users are empowered to manage the nature of their relationship with Engage Health via the service through a set of data controls. These allow the individual to express their preferences as detailed in ICO guidelines and under GDPR for how their data is stored, used and deleted.

Stakeholder engagement

The company engages with a number of stakeholders through various channels.

OPS users	Through direct contact via the service Patient Participation Groups (PPGs) NHS sponsored stakeholder forums
Healthcare professionals	User Groups Conferences Expert Groups
Customers	Project management teams
NHS arms / nations	Release Management team Program teams
Clinical system providers	Account management teams
Hosting provider (UK Cloud)	Account management Technical Architects
Security testing (Cyberis)	Account Management

Necessity and Proportionality

For OPS users, the lawful basis for processing is explicit consent (Articles 6.1.a and 9.2.a). Care is taken to ensure that the processing of special category data is clearly articulated to service users at multiple points of the user journey.

For Healthcare Professionals, the lawful basis is contractual with onward use typically covered by Articles 6.1.e and 9.2.h

Some audit data is covered by Legal Obligation and Public Task (Article 6.1.c)

Visibility of the data held and its use is given to all service users, with tools to exercise their rights over it wherever possible.

No data is directly shared with 3rd parties. Onward use of data that has been positively committed to National NHS systems by Healthcare Professionals that may be subject to use for research and

planning purposes is to be governed by citizen preference as set under the National Opt-Out model. Our services provide links to self-manage this.

The necessity to process and/or hold data is considered as part of the development process as outlined in the DEVxxx chapter of company policies.

Risk management

Each service component of the PSF has a "Security and IG Risk Management" folder where risks are identified, recorded and monitored. Risks are graded in accordance withSY109 - RIsk Management Policy, with sign-off by Senior Management and Company Executive required for Medium and High risks respectively.

These risk logs are under continual review and controlled in the main by the ISO27001 processes. Due to their frequent updates, they are not suitable for inclusion in this document, but (where appropriate) are available for inspection on request.

Governance

All documentation, processes and procedures will comply with company procedures, in particular SY401 - Information Governance.. The Company Executive is responsible for the maintenance and dissemination of this Impact Analysis.