

Schedule L – DPIA0018 – SCAS GP Encounter Data

Background & summary

This document provides a **Summary-level DPIA**. It should be read in conjunction with the sharing requirement specification for this data flow and the full DPIA created for the Azure-based Graphnet CareCentric analytics platform supporting Connected Care analytics and intelligence.

The document provides an assessment of the data protection and security impact of data flows from South Central Ambulance Service (SCAS) into the Connected Care platform. The data sets are based on the SCAS patient GP discharge summaries.

The local health and social care economies have identified improved intelligence regarding the local health and social care system as a priority. This is to be delivered through a strong analytics competency that can harness both personal and organisational (e.g. capacity, bed availability) data to create actionable caseloads, plans and insights, set future vision, improve outcomes and reduce the time required to deliver value to patients and professionals alike. The benefits of this capability include:

1. Timeliness of data. With access to near real-time dashboards there is the potential to rapidly and responsively reconfigure healthcare delivery across the health and social care community;
2. An extension of Connected Care's role as a single trusted repository of data for the whole system; and
3. System wide planning and modelling using consistent and commonly understood data sources.

The flow of patient discharge data sets from South Central Ambulance Service (SCAS) and the SCAS activity data into the Connected Care analytics and intelligence platform alongside near-real time A&E data as well as acute and community bed state reporting across hospitals in the ICS enhances the existing system status dashboard and will benefit operational teams by providing a more complete view of pathway and system utilisation, pressure points and capacity.

Benefits

The main benefit from sharing the patient discharge summary using the Connected Care platform is to enhance the existing patient longitudinal record which currently contains real time Primary Care GP data, secondary care data, mental health and community data. This results in a more complete understanding of patients' needs and will result in better:

1. Care planning;
2. Case finding, stratification and management; and
3. Discharge planning and the preparation of onward referrals.

The availability of this SCAS data is also expected to benefit the ICS and the wider population by enabling improved analysis of:

1. More complete profiles for emergency pathways;
2. Ambulance pathway planning;
3. Patient pathways and transfers by ambulance when the destination is somewhere other than A&E/hospital; and
4. Clinical scores, such as data items that feed into NEWS2 against outcomes and disposal methods.

While the analysis will be carried out on anonymous and pseudonymous data, in order to create these anonymous analysis views it is necessary to link the patient discharge data to the correct patients within the Connected Care analytics platform. As a consequence, identifiable patient discharge data sets are required.

What data is being used and how is it being used?

The categories of data extracted are drawn from the SCAS Patient Clinical Record (based on the specification of the "GP Report for Information V4.6.2"):

1. Patient Details;
2. Incident details;
3. History of presenting complaint;
4. Presenting Complaint;
5. Urinalysis;
6. Vital signs;
7. Medicines;
8. Social History; and
9. Safety Netting.

Schedule L – DPIA0018 – SCAS GP Encounter Data 2023 **SECONDARY USES** Information Sharing Agreement

An initial load of previous three years discharge summary data is proposed. The data will be limited to the resident population of the CCGs within the Connected Care footprint.

To ensure that only patients who are part of the Connected Care footprint are included, SCAS will only send information for patients who have a registered GP of one of the Connected Care CCG's (Gp practice is always taken from Spine connected computer systems) SCAS will never send any patient level information for patients who do not have an NHS number.

As indicated above, the Connected Care data is loaded into the Azure-based data warehouse and configured for use through the Connected Care Analytics data views (referred to as "Data Marts" here). These Data Marts are:

1. Data Mart 1 – **Identifiable data for use by** clinicians and social care professionals with a legitimate relationship and purpose, in particular in order to support case finding, referrals and the instigation or delivery of specific **direct care activity**. Data is only accessible through this Mart for users with a "professional" role as defined in User Access Profiles below;
2. Data Mart 2 – **Pseudonymised data** for use by individuals involved in the management of cohorts of service users, services themselves, pathways, etc. Data is only accessible through this Mart for users with "management" and "professional" roles as defined in User Access Profiles below; and
3. Data Mart 3, – **Fully anonymised data** for use in activities such as commissioning, modelling and planning. Data is accessible through this Mart for users with "commissioning", "management" and "professional" roles as defined in User Access Profiles below.

Who are the controllers of the data and who are the processors (if applicable)

South Central Ambulance Services are the controller. SoftCat Ltd is the processor for the Connected Care analytics and intelligence platform. In the SoftCat contract, SoftCat is the processor and the term for Graphnet (a "sub-processor" in law) in the contract is "actual processor". System C and Microsoft are also sub-processors.

Who has access to the data and how is that controlled?

There are four user access profiles in the role based access control (RBAC) model for the Connected Care analytics and intelligence platform. These are:

1. Professional – which provides access to Data Marts 1, 2 and 3 and permits the use of identifiable data:
 - a. For the purposes of this sharing requirement the data is expected to be used as part of this role by:
 - i. Referrers
 - ii. Case managers and care providers
 - iii. MDTs and integrated care teams
 - iv. Discharge teamsTo allow them reach more timely and informed decisions about patient care, referrals and dispositions;
2. Management – which provides access to Data Marts 2 and 3 and permits analysis using pseudonymous data:
 - a. The data made available under this sharing requirement and controlled through the Management role is expected to support analysis and decision making by:
 - i. Clinical directors
 - ii. ICS analysts
 - iii. Operational managers
 - iv. PCN managers
 - v. Service managers
 - vi. Service improvement teamsTo reach more timely and informed decisions about the design and operation of services and patient pathways;
3. Commissioning – which provides access to Data Mart 3 and permits analysis using anonymous data:
 - a. For the purposes of this sharing requirement there is no Commissioning user requirement; and
4. Administrator – which is used to control access and define analyses.

For users accessing the PowerBi Connected Care portal where access to data is controlled using role- based access (RBAC).

Schedule L – DPIA0018 – SCAS GP Encounter Data 2023 **SECONDARY USES** Information Sharing Agreement

All SQL and PowerBi reporting access is controlled at row level ensuring that users only ever see the data they are supposed to. No patient identifiable data is ever made available to users without the correct privileges and authorisation.

With regards to gaining access to the platform, all Graphnet support staff and customer accounts are tracked with an account request created in the Graphnet Connected Care Jira service desk. Jira generates a full audit trail of all requests and actions. Any user request is reviewed and delivered by our administration team who will deliver a profile set up in line with the role, products needed.

Accounts for Customers to access the BI platform

Customer account requests can only be raised by an already authorised employee from the Connected Care organisation inside their existing Jira service desk.

1. Customer ITIL service desk accounts for issue logging, follow a standardised roll out to allow staff to create and manage service desk tickets in their service desk for the products purchased; and
2. Cloud Access Service desks (where in use); require the request creator to specify exactly which security roles to attribute to the new Power BI user account.

Internal staff accounts to access the BI platform for support and maintenance reasons

Graphnet manage staff access within Jira service desks and all network facilities in line with GN BMS-DOC 013 Access Control policy as part of their ongoing ISO/IEC 27001:2013 certification:

1. Access provided is based on “least privilege” best practice in line with their role; and
2. Access is reviewed as part of regular access audit and is reassessed if staff move roles or change the clients they are servicing.

Has the DPIA identified appropriate lawful basis to share and whether any sharing documentation is required?

The lawful basis is the “exercise of official authority”, “the provision of health or social care or treatment” and the “management of health and care services”. The common law duty of confidentiality is respected as the processing of the data is performed using anonymous or pseudonymous views of the data.

Summary of the risks, issues and proposed mitigation from the DPIA:

The primary risks associated with this data flow are:

1. The security of the data transfer process:
 - a. The configuration of the destination address is reviewed by the SCAS and Graphnet technical and security teams to ensure that the data is delivered to the correct destination
 - b. The security of the destination address has been assessed as part of the overall Connected Care Azure platform DPIA completed by the Connected Care team and approved previously by the IGSG;
2. The security of the data access arrangements and the data storage arrangements:
 - a. This is managed through role based access controls (RBAC)
 - b. The RBAC arrangements have been tested as part of the Connected Care analytics platform proof of concept
 - c. The RBAC arrangements have been assessed as part of the overall Connected Care Azure platform DPIA completed by the Connected Care team and approved previously by the IGSG; and
3. The accuracy of the matching of the patient-level data:
 - a. The patient level data is matched using NHS number
 - b. [The NHS number match is confirmed using the patient surname/address/data of birth?].

End of Schedule L