Prescribing Services

ADVICE AND GUIDANCE

Data Protection by Design

VERSION DATE	NOTES	AUTHOR
2021-09-24	Redraft. Previous versions available at PSL DPIA	Emma Cooper, Kafico Ltd

KAFICO

INFORMATION · GOVERNANCE · CONSULTANCY

1. PROJECT CONTEXT

Eclipse Vista

Our NHS is very active implementing new clinical pathways, projects and initiatives. However, NHS organisations are far less effective at measuring the impact of these implementations. The VISTA Pathways interface has been specifically designed for CCGs and their GP Practices to enable effective validation of these implementations. It provides NHS organisations with a highly focused and effective population health management tool. VISTA Pathways brings together a region's Advice & Guidance (Eclipse Live) Primary Care data and their SUS+ Secondary Care utilisation data. The result is a complete validation solution allowing patient cohorts associated with a clinical pathway, project or initiative to be selected and their associated costs to be reviewed and validated.

The analytical and validating functionality within VISTA Pathways provides NHS Organisations with a highly effective population segmentation, planning and validation solution.

By triangulating the Advice & Guidance (Eclipse Live) Primary Care patient data, national prescribing data and NHS Digital SUS+ data within a secure platform VISTA Pathways enables NHS organisations to:

1. Define any patient cohort.
2. Plan and model any implementations needed for this cohort.
3. Track the adherence to the desired implementation.
4. Validate the full impact of this implementation upon the patient cohort.
5. Evaluate the benefit of continuing the clinical pathway, project or initiative.

2. DATA FLOWS

NHS Pathways / Eclipse / Advice and Guidance / VISTA

The initial uploads can either be manual or automated as described below. This is the decision of the GP Practice.

GP Data is extracted with nationally identified sensitive read codes removed (as specified by ISB-1572). This creates datasets containing only de-identified data used for data analysis. This data is fully encrypted to allow secure transmission of data to our high security data centre using AES 256bit encryption.

Manual Uploads

1. Primary care data sets (Practice Code, Patient Reference / MiQuest, Number, Gender, Age in Years, Medication issue date, medication type (acute, repeat), Medication directions, code date, clinical code, code description, result 1 & result 2) are created from primary care system reporting tools, MiQuest and EMIS Population manager.
2. The data sets are then transmitted directly from the practice using Eclipse website using TLS1.1, 1.2 secure socket connections.

Automated Uploads

1. Primary care data sets (Practice Code, Patient Reference / MiQuest, Number, Gender, Age in Years, Medication issue date, medication type (acute, repeat), Medication directions, code date, clinical code, code description, result 1 & result 2) are created from bulk data extracts directly at practice by Apollo SQL Suite.
2. Transmitted directly from practice over AES-256bit web services.

The remaining data flows describe the process regardless of the upload method.

3. Upon landing in the PSL hosting facilities, a numeric identifier (Eclipse Identifier) is created for each patient. Data is summarised and stored for use with web-based applications.
4. This pseudonymised primary care data, with only internal practice identifier, is now held in NHSD certified, tested, approved data centre in disused nuclear bunker.
5. A ‘Little Gemini’ data set (Patient File, Practice Code, Patient reference / MiQuest Number, NHS Number) is created from primary care system reporting tools, MiQuest and EMIS Population manager. File is encrypted using AES-256bit encryption.
6. Transmitted as data directly from practice using Eclipse website hosted within the HSCN network using TLS1.1, 1.2 secure socket connections.
7. Upon landing in the PSL hosting facilities, the practice Code and patient reference in the Little Gemini data set are used to find the Eclipse Identifier for each patient within the dataset. The Eclipse identifier along with the encrypted (AES 256) patient

identifiable information are transmitted over a secure encrypted tunnel to the Trusted 3rd Party server hosted within the HSCN network at a local hospital.

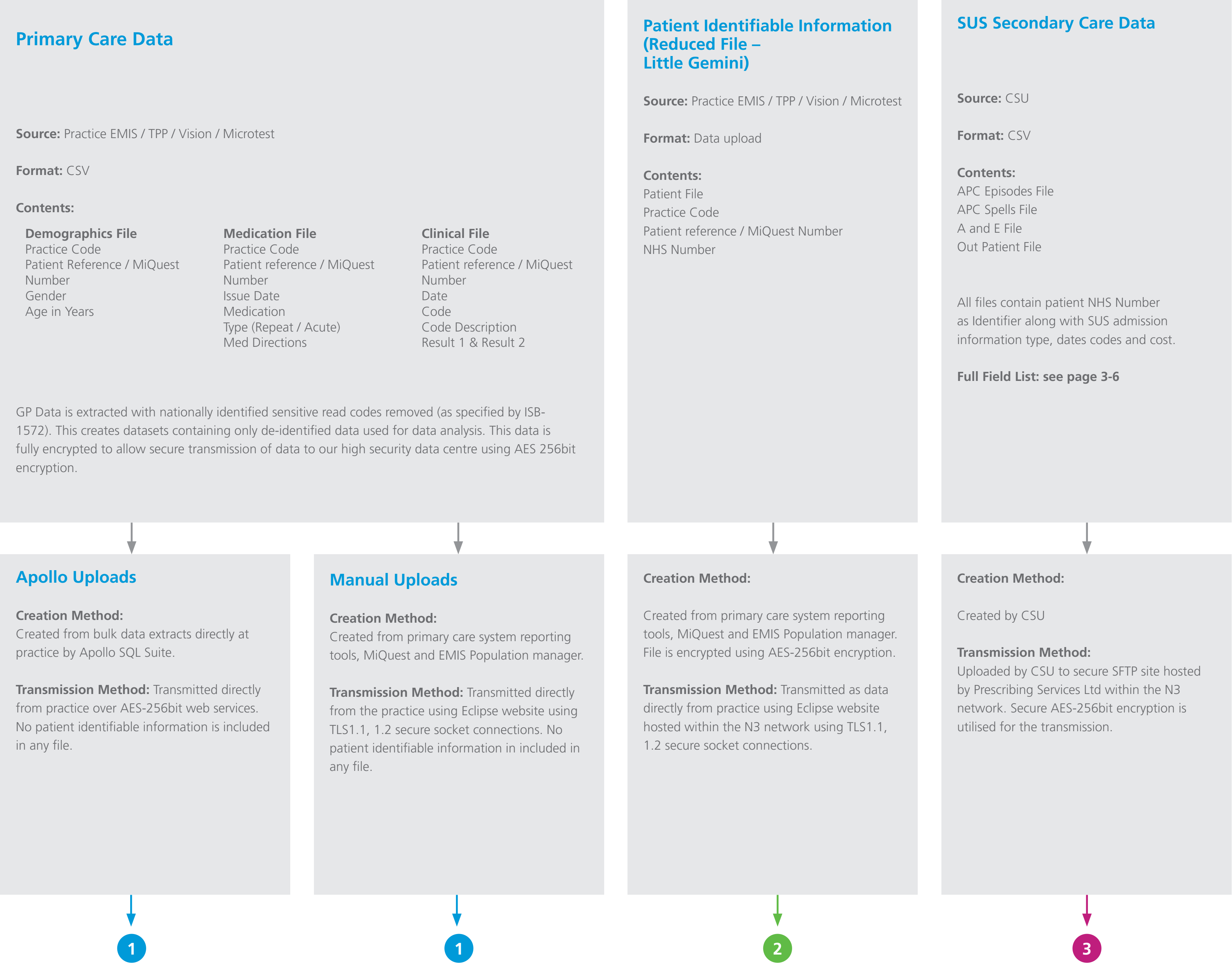
8. SUS Secondary care data sets (APC Episodes File, APC Spells File, A and E File, Out Patient File) are created by the CSU. All files contain patient NHS Number as Identifier along with SUS admission information type, dates codes and cost. Full fields available in diagram below.
9. Uploaded by CSU to secure SFTP site hosted, by Prescribing Services Ltd within the HSCN, network. Secure AES-256bit encryption is utilised for the transmission.
10. 1Upon landing in the PSL hosting facilities, Data arrives through secure channels to a monitored folder in the PSL hosting facilities. When files are detected they are processed instantly.
11. Steps:
    - ✓ Files are read into memory.
    - ✓ For each line of the file the NHS Number is read into memory, encrypted and transmitted using AES encrypted channels to the QUHKL server.
    - ✓ The QUEKL server compares the ciphertext to encrypted NHS Numbers stored.
    - ✓ Where a match is found, the Eclipse Identifier is returned
    - ✓ The NHS Number is removed from the file line and replaced with the Eclipse Identifier.
    - ✓ Data is stored de-identified in a secure SQL Server
    - ✓ Files are permanently deleted.
12. De-identified SUS, data linked using derived Eclipse identifier, is now held in NHSD certified, tested, approved data centre in disused nuclear bunker.
13. User access to web-based application which uses Microsoft technologies (ASP.Net and SQL Server).
14. Access is limited to authorised users and utilises role-based access using 2 factor authentication.
15. Utilises primary care data and SUS Data which is pseudonymised for practice users who can only use the available patient reference for identification of patients with access to their own primary care system.
16. Practices that are using ‘Little Gemini’ can perform reidentification of patients raised via patient alerts and long-term condition manager.
17. This allows an authorised user to request display the NHS Number .

18. This sends the Eclipse identifier to the QEHKL to search for patient information. Where found an encrypted NHS number is returned and displayed in a separate window. The NHS number is not stored or cached and all access logged.
19. Presentation of the NHS Number can only be performed when accessed via a secure HSCN connection.
20. All user details are de-identified for use by the CCG.

Note: in the diagram below, reference to N3 should be read as HSCN.

Prescribing Services

Prescribing Services Ltd Data Flow



Primary Care Data

Source: Practice EMIS / TPP / Vision / Microtest

Format: CSV

Contents:

Demographics File
Practice Code
Patient Reference / MiQuest Number
Gender
Age in Years

Medication File
Practice Code
Patient reference / MiQuest Number
Issue Date
Medication
Type (Repeat / Acute)
Med Directions

Clinical File
Practice Code
Patient reference / MiQuest Number
Date
Code
Code Description
Result 1 & Result 2

GP Data is extracted with nationally identified sensitive read codes removed (as specified by ISB-1572). This creates datasets containing only de-identified data used for data analysis. This data is fully encrypted to allow secure transmission of data to our high security data centre using AES 256bit encryption.

Patient Identifiable Information (Reduced File – Little Gemini)

Source: Practice EMIS / TPP / Vision / Microtest

Format: Data upload

Contents:
Patient File
Practice Code
Patient reference / MiQuest Number
NHS Number

SUS Secondary Care Data

Source: CSU

Format: CSV

Contents:
APC Episodes File
APC Spells File
A and E File
Out Patient File

All files contain patient NHS Number as Identifier along with SUS admission information type, dates codes and cost.

Full Field List: see page 3-6

Apollo Uploads

Creation Method:
Created from bulk data extracts directly at practice by Apollo SQL Suite.

Transmission Method: Transmitted directly from practice over AES-256bit web services. No patient identifiable information is included in any file.

1

Manual Uploads

Creation Method:
Created from primary care system reporting tools, MiQuest and EMIS Population manager.

Transmission Method: Transmitted directly from the practice using Eclipse website using TLS1.1, 1.2 secure socket connections. No patient identifiable information in included in any file.

1

Creation Method:

Created from primary care system reporting tools, MiQuest and EMIS Population manager. File is encrypted using AES-256bit encryption.

Transmission Method: Transmitted as data directly from practice using Eclipse website hosted within the N3 network using TLS1.1, 1.2 secure socket connections.

2

Creation Method:

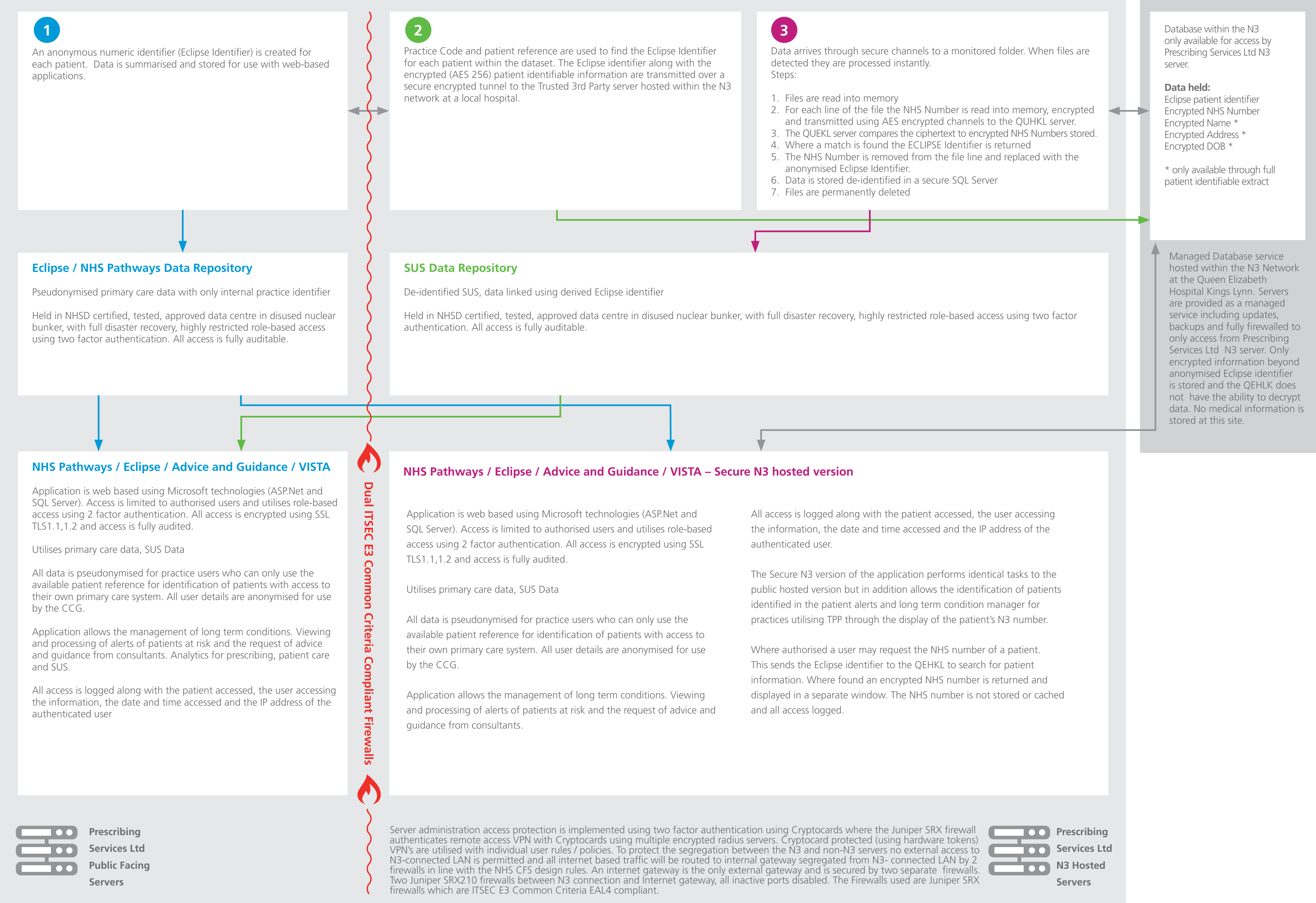
Created by CSU

Transmission Method:
Uploaded by CSU to secure SFTP site hosted by Prescribing Services Ltd within the N3 network. Secure AES-256bit encryption is utilised for the transmission.

3

Prescribing Services LTD Hosting Facilities

QEHKL Server



1

An anonymous numeric identifier (Eclipse Identifier) is created for each patient. Data is summarised and stored for use with web-based applications.

2

Practice Code and patient reference are used to find the Eclipse Identifier for each patient within the dataset. The Eclipse identifier along with the encrypted (AES 256) patient identifiable information are transmitted over a secure encrypted tunnel to the Trusted 3rd Party server hosted within the N3 network at a local hospital.

3

Data arrives through secure channels to a monitored folder. When files are detected they are processed instantly.
Steps:

1. Files are read into memory
2. For each line of the file the NHS Number is read into memory, encrypted and transmitted using AES encrypted channels to the QUHKL server.
3. The QUEKL server compares the ciphertext to encrypted NHS Numbers stored.
4. Where a match is found the ECLIPSE Identifier is returned
5. The NHS Number is removed from the file line and replaced with the anonymised Eclipse Identifier.
6. Data is stored de-identified in a secure SQL Server
7. Files are permanently deleted

Database within the N3 only available for access by Prescribing Services Ltd N3 server.

Data held:
Eclipse patient identifier
Encrypted NHS Number
Encrypted Name *
Encrypted Address *
Encrypted DOB *

* only available through full patient identifiable extract

Managed Database service hosted within the N3 Network at the Queen Elizabeth Hospital Kings Lynn. Servers are provided as a managed service including updates, backups and fully firewalled to only access from Prescribing Services Ltd N3 server. Only encrypted information beyond anonymised Eclipse identifier is stored and the QEHLK does not have the ability to decrypt data. No medical information is stored at this site.

Eclipse / NHS Pathways Data Repository

Pseudonymised primary care data with only internal practice identifier

Held in NHSD certified, tested, approved data centre in disused nuclear bunker, with full disaster recovery, highly restricted role-based access using two factor authentication. All access is fully auditable.

SUS Data Repository

De-identified SUS, data linked using derived Eclipse identifier

Held in NHSD certified, tested, approved data centre in disused nuclear bunker, with full disaster recovery, highly restricted role-based access using two factor authentication. All access is fully auditable.

NHS Pathways / Eclipse / Advice and Guidance / VISTA

Application is web based using Microsoft technologies (ASP.Net and SQL Server). Access is limited to authorised users and utilises role-based access using 2 factor authentication. All access is encrypted using SSL TLS1.1,1.2 and access is fully audited.

Utilises primary care data, SUS Data

All data is pseudonymised for practice users who can only use the available patient reference for identification of patients with access to their own primary care system. All user details are anonymised for use by the CCG.

Application allows the management of long term conditions. Viewing and processing of alerts of patients at risk and the request of advice and guidance from consultants. Analytics for prescribing, patient care and SUS.

All access is logged along with the patient accessed, the user accessing the information, the date and time accessed and the IP address of the authenticated user

Dual ITSEC E3 Common Criteria Firewalls

NHS Pathways / Eclipse / Advice and Guidance / VISTA – Secure N3 hosted version

Application is web based using Microsoft technologies (ASP.Net and SQL Server). Access is limited to authorised users and utilises role-based access using 2 factor authentication. All access is encrypted using SSL TLS1.1,1.2 and access is fully audited.

Utilises primary care data, SUS Data

All data is pseudonymised for practice users who can only use the available patient reference for identification of patients with access to their own primary care system. All user details are anonymised for use by the CCG.

Application allows the management of long term conditions. Viewing and processing of alerts of patients at risk and the request of advice and guidance from consultants.

All access is logged along with the patient accessed, the user accessing the information, the date and time accessed and the IP address of the authenticated user.

The Secure N3 version of the application performs identical tasks to the public hosted version but in addition allows the identification of patients identified in the patient alerts and long term condition manager for practices utilising TPP through the display of the patient’s N3 number.

Where authorised a user may request the NHS number of a patient. This sends the Eclipse identifier to the QEHKL to search for patient information. Where found an encrypted NHS number is returned and displayed in a separate window. The NHS number is not stored or cached and all access logged.

Prescribing Services Ltd Public Facing Servers

Server administration access protection is implemented using two factor authentication using Cryptocards where the Juniper SRX firewall authenticates remote access VPN with Cryptocards using multiple encrypted radius servers. Cryptocard protected (using hardware tokens) VPN’s are utilised with individual user rules / policies. To protect the segregation between the N3 and non-N3 servers no external access to N3-connected LAN is permitted and all internet based traffic will be routed to internal gateway segregated from N3- connected LAN by 2 firewalls in line with the NHS CFS design rules. An internet gateway is the only external gateway and is secured by two separate firewalls. Two Juniper SRX210 firewalls between N3 connection and Internet gateway, all inactive ports disabled. The Firewalls used are Juniper SRX firewalls which are ITSEC E3 Common Criteria EAL4 compliant.

Prescribing Services Ltd N3 Hosted Servers

Admitted Patient Care (APC) Episodes Fields

SUS Version
NHS RID (From Provider)
Generated Record ID
CDS Record Type
Reason Access Provided
CDS Group Derived
CDS Group Indicator
Bulk Replacement CDS Group
Pseudonymised Status
Confidentiality Category
NHS Number
Lead Care Activity Indicator
RTT Period End Date
RTT Period Start Date
RTT Status
Unique Booking Reference Number (Converted)
RTT Length (Derived)
Age At CDS Activity Date
Patient Type
Age at Start of Episode Derived
Age At Start of Spell
Spell Age
Episode Age
Year of Birth
Birth Month
Age at Spell End Original
Age at Record Start
Age At End of Spell
Age at Spell Start Original
Age at Record End
Age Range Derived
Age Range Derived (Mother)
Carer Support Indicator
Legal Status Classification Code
Ethnic Category Code
Marital Status
NHS Number Status Indicator
Gender Code
Total Previous Pregnancies
Postcode Sector of Usual Address
Organisation Code (PCT of Residence)
Patient Postcode Derived PCT Type
Patient Postcode Derived PCT
Organisation Code Type PCT of Residence
Area Code of Usual Address
Area Code Derived
Organisation Code (PCT of Residence - Mother)
Patient Postcode Derived PCT Type (Mother)
Patient Postcode Electoral Ward
SHA Type from Patient Postcode
Census Output Area 2001
Country
County Code
ED County Code
ED District Code
Electoral Ward Division
Government Office Region Code
Local Authority Code
SHA Old Org Code
Electoral Ward 1998
Hospital Provider Spell No
ADMINISTRATIVE CATEGORY (AT START OF EPISODE)
ADMINISTRATIVE CATEGORY (ON ADMISSION)
Patient Classification
Admission Method (Hospital Provider Spell)
Admission Method (Original Data)
Admission Type (Derived)
Admission Subtype (Derived)
Discharge Destination (Hospital Provider Spell)
Discharge Method (Hospital Provider Spell)
Source of Admission (Hospital Provider Spell)
Start Date (Hospital Provider Spell)
End Date (Hospital Provider Spell)
Spell In PbR/Not In PbR
Spell Version As At Date And Time
Delay Discharge Reason
Delayed Discharged Days
Administrative Category (Derived)
Elective Admission Type

PbR Spell Start Date
PbR Spell End Date
Hospital Provider Spell Discharge Date
Hospital Provider Spell End Date
Ready for Discharge Date
PbR Delayed Discharge Days Derived
Spell Exclusion Reason
Applicable Costing Period
Episode Number
First Regular Day Night Admission
Last Episode in Spell Indicator
Neonatal Level of Care
Operation Status
Episode Start Date
Episode End Date
CDS Activity Date
Episode Start Date Original
Commissioner Serial No (Agreement No)
NHS Service Agreement Line No
Provider Reference No
Commissioner Reference No
SHA Commissioner
SHA Provider
Organisation Code (Code of Provider)
Provider Site Code
Organisation Code (Code of Commissioner)
Commissioner Code (Original Data)
Commissioner Site Code
Spell Commissioner Code
PCT Derived from GP
PCT Derived from GP Practice
GP Practice Derived from PDS
Site code of Treatment (at start of episode)
Organisation Code Type Provider
Provider Code (Original Data)
Provider Location Derived
Organisation Code Type Commissioner
GP PCT Type (Derived)
SHA from GP (Derived)
SHA Type from GP (Derived)
PCT Derived from GP Practice (Mother)
Consultant Code
Main Specialty Code
Treatment Function Code
Consultant Code Type
Consultant Organisation Code
Organisation Code Type Consultant
Specialty Function Code Original
Elective Consultant Code
Elective Consultant Specialty Code
Elective Consultant Code Type
Elective Specialty Function Code
Elective Consultant Organisation Code
Organisation Code Type Elective Consultant
Antenatal Consultant Code
Antenatal Consultant Specialty Code
Antenatal Consultant Code Type
Antenatal Specialty Function Code
Antenatal Consultant Organisation Code
Organisation Code Type Antenatal Consultant
Registered GMP Code
GP Code (Original data)
GP Practice Code
GP Consortium Code
GP Practice Code (Original Data)
GP Practice Code (Derived)
Referrer Code
Referring Organisation Code
Code of GP
Organisation Code GP
Organisation Code Type GP
Organisation Code Type GP Practice
GP Code (Mother)
Organisation Code GP (Mother)
Organisation Code Type GP (Mother)
GP Code Type
GP Code Type (Mother)
First GP Organisation Code
GP Practice Code Original
GP Practice Code Derived
GP Practice Code derived (Mother)
Organisation Code Type Referrer
Referrer Code Type
Organisation Code Type Prime Recipient

Duration of Elective Wait
Intended Management
Decided To Admit Date
Episode Duration
Episode Duration Grouper
Length of Stay (Hospital Provider Spell)
PbR NCC PCC Adjusted Length of Stay
PbR Final Adjusted Length of Stay
Spell ACC Length Of Stay
Spell NCC Length Of Stay
Spell PCC Length Of Stay
Spell Primary Diagnosis
Spell Secondary Diagnosis
HRG Submitted
HRG Version (Submitted)
Core HRG (Calculated)
Episode HRG Version (Calculated)
Episode Dominant Procedure
Grouping Algorithm Version
Grouping Reference Data Version
Grouping HRG Version
Spell Core HRG
HRG Dominant Grouping Variable
HRG Procedure Scheme
Unbundled HRG 1
Unbundled HRG 2
Unbundled HRG 3
Unbundled HRG 4
Unbundled HRG 5
Unbundled HRG 6
Unbundled HRG 7
Unbundled HRG 8
Unbundled HRG 9
Unbundled HRG 10
Unbundled HRG 11
Unbundled HRG 12
Programme Budgeting Category
Spell Programme Budgeting Category
Spell Report Flag
PbR Excluded Indicator
Episode Exclusion Reason
Code Cleaning
PbR Costed Indicator
Grouping Method
Configurable Indicator
Diagnosis Scheme In Use
Primary Diagnosis Code
Secondary Diagnosis Code 1
Secondary Diagnosis Code 2
Secondary Diagnosis Code 3
Secondary Diagnosis Code 4
Secondary Diagnosis Code 5
Secondary Diagnosis Code 6
Secondary Diagnosis Code 7
Secondary Diagnosis Code 8
Secondary Diagnosis Code 9
Secondary Diagnosis Code 10
Secondary Diagnosis Code 11
Secondary Diagnosis Code 12
Procedure Scheme In Use
Primary Procedure Code
Primary Procedure Date
Secondary Procedure Code 1
Secondary Procedure Date 1
Secondary Procedure Code 2
Secondary Procedure Date 2
Secondary Procedure Code 3
Secondary Procedure Date 3
Secondary Procedure Code 4
Secondary Procedure Date 4
Secondary Procedure Code 5
Secondary Procedure Date 5
Secondary Procedure Code 6
Secondary Procedure Date 6
Secondary Procedure Code 7
Secondary Procedure Date 7
Secondary Procedure Code 8
Secondary Procedure Date 8
Secondary Procedure Code 9
Secondary Procedure Date 9
Secondary Procedure Code 10
Secondary Procedure Date 10
Secondary Procedure Code 11
Secondary Procedure Date 11
Secondary Procedure Code 12

Secondary Procedure Date 12
Spell Dominant Procedure
Advanced Cardiovascular Support Days
Advanced Respiratory Support Days
Basic Cardiovascular Support Days
Basic Respiratory Support Days
Critical Care Level 2 Days
Critical Care Level 3 Days
Critical Care Unit Function
Dermatological Support Days
Neurological Support Days
Renal Support Days
Liver Support Days
Episode ACC Length Of Stay
Episode NCC Length Of Stay
Episode PCC Length Of Stay
APC Tariff ID
Market Forces Factor
Market Forces Factor ID
Tariff Initial Amount National
Tariff Day Case National
Tariff Long Stay Payment National
Tariff Long Stay Rate National
Tariff Service Adjustment National
Tariff Short Stay Elective National
Tariff Short Stay Emergency National
Aggregate UnBundled Adjustment National
Tariff Financial Adjustment National
Tariff Adjustment Future Use_1 National
Tariff Adjustment Future Use_2 National
Applied MFF Elective
Applied MFF Non Elective
MFF Adjustment
Tariff Pre MFF Adjusted National
Tariff Total Payment National
Tariff Initial Amount Non Mandatory
Tariff Day Case Non Mandatory
Tariff Short Stay Emergency Non Mandatory
Tariff Spec Serv Adjustment Non Mandatory
Tariff Long Stay Rate Non Mandatory
Tariff Long Stay Payment Non Mandatory
Aggregate UnBundled Adjustment Non Mandatory
Tariff Financial Adjustment Non Mandatory
Tariff Adjustment Future Use_1 Non Mandatory
Tariff Adjustment Future Use_2 Non Mandatory
Applied MFF Elective Non Mandatory
Applied MFF Non Elective Non Mandatory
Tariff Pre MFF Adjusted Non Mandatory
Tariff Total Payment Non Mandatory
Non Mandatory Core Tariff (with UB)
Optional APC BPT Adjustment
Tarrif Initial Amount Local
Tariff Day Case Local
Tariff Short Stay Emergency Local
Tariff Long Stay Rate Local
Aggregate UnBundled Adjustment Local
Tariff Long Stay Payment Local
Tariff Total Payment Local
Local Core Tariff (with UB)
PbR Final Tariff
Final Tariff Applied
App Period Spell Status Indicator
Hospital Provider Spell Duration Days Derived
Number of Episodes in PbR Spell
RAP DH Tariff Adjustment Child
RAP Validation Child Indicator
RAP Spell Type
PbR Generated Interchange ID
PbR Spell Cost ID
PbR Spell Cost Version Date
PbR Spell Const Version Number
PbR Spell Complete Indicator
PbR Spell Error Status
PbR Spell Frozen Indicator
Spell Service ID
Spell Service Version
PbR Spell Status Indicator
Match Criterion Indicator
Number of Babies
Location Class of Delivery Place (Intended)
Location Type of Delivery Place (Intended)

Anaesthetic During Labour
Anaesthetic Post Labour
Location Class of Delivery Place (Actual)
Location Type of Delivery Place (Actual)
Birth Order
Birth Weight
Delivery Method
Delivery Place Change Reason
Delivery Place Type Actual
Delivery Place Type Intended
First Antenatal Assessment Date
Gestation Length
Gestation Length Assessment
Live or Still Birth
Status of Person Conducting Delivery
NHS Number Status Ind (Baby)
Sex (Baby)
Costing Batch Sequence
Count of Days Suspended
Current Period Number
PbR Days Beyond Trimpoint
PbR Spell Trimpoint Days
Significant Specialised Service Code
Specialised Service Code 1
Specialised Service Code 2
Specialised Service Code 3
Specialised Service Code 4
Specialised Service Code 5
BPT Indicator 1
BPT Indicator 1 Action
BPT Indicator 2
BPT Indicator 2 Action
BPT Indicator 3
BPT Indicator 3 Action
BPT Indicator 4
BPT Indicator 4 Action
BPT Indicator 5
BPT Indicator 5 Action
Episode Duration Days Derived
Error Reason
Excluded Critical Care Days
Finished Indicator
First Attendance
First Staging Loaded Date
HES Identifier
Hierarchy
Intended Procedure Status
Interchange ID
Last Did Not Arrive Date
Last Entry Review Date
Last Staging Loaded Date
Location Type Code
Logically Deleted Date
Maximum Episode Date
Onset Method
Organisation Code Type Location
Other Indicator
Outcome Of Attendance
PCT Responsible
Record Extraction Indicator
Re-costing Requested Flag
Resuscitation Method
Service Original
Service Top-up Percentage
Short Stay Redn Pcnt
Significant Service ID
Specialty Service Top-up
Temporary Cost Period Status
Test Indicator
Update Type
Version Sequence Number
Number of Commissioners in PbR Spell
Number Diagnosis
Number Procedures
Number Unbundled HRGs
Number Unbundled Non Priced HRGs
Number Unbundled Priced HRGs
Excluded Episodes in Hospital Provider Spell
Number Hospital Provider Spell ID
Number SSCs
Number BPT Indicators
Organisation Code (Sender)
Staging Loaded Date
Protocol Identifier
Unique CDS Identifier

Applicable Date
Extract Date
Report Period Start Date
Report Period End Date
Organisation Code Type Sender
Dominant Staging Loaded Date
Extract Type
Location Class at Epistart
Org Code Location at Epistart
Org Code Type Location at Epistart
Intended Care Intensity at Epistart
Age Group Intended at Epistart
Sex Of Patients at Epistart
Day Period Availability at Epistart
Night Period Availability at Epistart
Location Class at Epiend
Org Code Location at Epiend
Org Code Type Location at Epiend
Intended Care Intensity at Epiend
Age Group Intended at Epiend
Sex Of Patients at Epiend
Day Period Availability at Epiend
Night Period Availability at Epiend
Spare 1
Spare 2
Spare 3
Spare 4
Spare 5
FCE NPOC
FCE Service Line
FCE Service Line List
Spell NPOC
Spell Service Line
Commissioning Region
Data Quality Indicator
Unbundled exclusion reason
CDS Schema Version
Query Date
Unique Query Id
Prime Recipient
Copy Recipients
Ward Code at Episode Start Date
Ward Security Level at Episode Start Date
Ward Code at Episode End Date
Ward Security Level at Episode End Date
Derived Commissioner
Derived Commissioner Type
Open Spell Indicator
NHSE Planning Commissioner

Admitted Patient Care (APC) Spells Fields

- SUS Version
- Pseudonymised Status
- Reason Access Provided
- NHS Number
- RTT Period End Date
- RTT Period Start Date
- RTT Status
- Unique Booking Reference Number (Converted)
- Age At CDS Activity Date
- Age At Start of Spell
- Age At End of Spell
- Spell Age
- Patient Type
- Carer Support Indicator
- Legal Status Classification Code
- Ethnic Category Code
- Marital Status
- NHS Number Status Indicator
- Gender Code
- Organisation Code (PCT of Residence)
- Patient Classification
- Admission Type (Derived)
- Admission Subtype (Derived)
- Ready for Discharge Date
- Delay Discharge Reason
- Spell In PbR/Not In PbR
- Spell Exclusion Reason
- Spell Version As At Date And Time
- Applicable Costing Period
- Provider Reference No
- Commissioner Reference No
- SHA Commissioner
- SHA Provider
- Organisation Code (Code of Provider)
- Provider Code (Original Data)
- Provider Site Code
- Organisation Code (Code of Commissioner)
- Commissioner Code (Original Data)
- Commissioner Site Code
- Organisation Code Type Commissioner
- PCT Derived from GP
- PCT Derived from GP Practice
- GP Practice Derived from PDS
- Main Specialty Code
- Treatment Function Code
- Registered GMP Code
- GP Code (Original data)
- GP Practice Code
- GP Consortium Code
- GP Practice Code (Original Data)
- GP Practice Code (Derived)
- Organisation Code Type GP Practice
- Referrer Code
- Referring Organisation Code
- Duration of Elective Wait
- Intended Management
- Decided To Admit Date
- Length of Stay (Hospital Provider Spell)
- PbR NCC PCC Adjusted Length of Stay
- PbR Final Adjusted Length of Stay
- Number of Commissioners in PbR Spell
- Number Diagnosis
- Number Hospital Provider Spell ID
- Number Procedures
- Number Unbundled HRGs
- Number Unbundled Non Priced HRGs
- Number Unbundled Priced HRGs
- Excluded Episodes in Hospital Provider Spell
- Number SSCs
- Number BPT Indicators
- PbR Spell Trimpoint Days
- PbR Days Beyond Trimpoint
- Spell ACC Length Of Stay
- Spell NCC Length Of Stay
- Spell PCC Length Of Stay
- Spell Primary Diagnosis
- Spell Secondary Diagnosis
- Spell Dominant Procedure
- Primary Procedure Code
- Significant Specialised Service Code
- Specialised Service Code 1
- Specialised Service Code 2
- Specialised Service Code 3
- Specialised Service Code 4
- Specialised Service Code 5
- BPT Indicator 1
- BPT Indicator 1 Action
- BPT Indicator 2
- BPT Indicator 2 Action
- BPT Indicator 3
- BPT Indicator 3 Action
- BPT Indicator 4
- BPT Indicator 4 Action
- BPT Indicator 5
- BPT Indicator 5 Action
- Tariff Initial Amount National
- Tariff Day Case National
- Tariff Short Stay Emergency National
- Tariff Service Adjustment National
- Tariff Long Stay Rate National
- Tariff Long Stay Payment National
- Aggregate UnBundled Adjustment National
- Tariff Financial Adjustment National
- Tariff Adjustment Future Use_1 National
- Tariff Adjustment Future Use_2 National
- Applied MFF Elective
- Applied MFF Non Elective
- MFF Adjustment
- Tariff Pre MFF Adjusted National
- Tariff Total Payment National
- Tariff Initial Amount Non Mandatory
- Tariff Day Case Non Mandatory
- Tariff Short Stay Emergency Non Mandatory
- Tariff Spec Serv Adjustment Non Mandatory
- Tariff Long Stay Rate Non Mandatory
- Tariff Long Stay Payment Non Mandatory
- Aggregate UnBundled Adjustment Non Mandatory
- Tariff Financial Adjustment Non Mandatory
- Tariff Adjustment Future Use_1 Non Mandatory
- Tariff Adjustment Future Use_2 Non Mandatory
- Applied MFF Elective Non Mandatory
- Applied MFF Non Elective Non Mandatory
- Tariff Pre MFF Adjusted Non Mandatory
- Tariff Total Payment Non Mandatory
- Non Mandatory Core Tariff (with UB)
- Optional APC BPT Adjustment
- Tarrif Initial Amount Local
- Tariff Day Case Local
- Tariff Short Stay Emergency Local
- Tariff Long Stay Rate Local
- Aggregate UnBundled Adjustment Local
- Tariff Long Stay Payment Local
- Tariff Total Payment Local
- Local Core Tariff (with UB)
- PbR Final Tariff
- Final Tariff Applied
- PbR Costed Indicator
- Grouping Method
- Configurable Indicator
- Code Cleaning
- Spell Core HRG
- Core HRG Version (Calculated)
- HRG Submitted
- HRG Version (Submitted)
- Grouping Algorithm Version
- Grouping Reference Data Version
- Grouping HRG Version
- Unbundled HRG 1
- Unbundled HRG 2
- Unbundled HRG 3
- Unbundled HRG 4
- Unbundled HRG 5
- Unbundled HRG 6
- Unbundled HRG 7
- Unbundled HRG 8
- Unbundled HRG 9
- Unbundled HRG 10
- Unbundled HRG 11
- Unbundled HRG 12
- Spell Programme Budgeting Category
- Number of Babies
- PbR Spell Error Status
- PbR Spell Frozen Indicator
- PbR Spell Status Indicator
- Match Criterion Indicator
- RAP DH Tariff Adjustment Child
- RAP Validation Child Indicator
- RAP Spell Type
- Applicable Date
- Extract Date
- Extract Type
- Spare 1
- Spare 2
- Spare 3
- Spare 4
- Spare 5
- Spell NPOC
- Spell Service Line
- Commissioning Region
- CDS Schema Version
- Query Date
- Unique Query Id
- Prime Recipient
- Copy Recipients
- Derived Commissioner
- Derived Commissioner Type
- Open Spell Indicator

Out Patient Appiontment Fields

SUS Version
NHS RID (From Provider)
CDS Record Type
Reason Access Provided
CDS Group Derived
CDS Group Indicator
Bulk Replacement CDS Group
Exclusion Reason
Pseudonymised Status
Confidentiality Category
Configurable Indicator
Code Cleaning
NHS Number
Lead Care Activity Indicator
RTT Period End Date
RTT Period Start Date
RTT Status
Unique Booking Reference Number (Converted)
RTT Length (Derived)
Age
Derived Age
Patient Type
Year of Birth
Month of Birth
Age at Record End
Age at Record Start
Age Range Derived
Carer Support Indicator
Ethnic Category Code
Marital Status
NHS Number Status Indicator
Gender Code
Postcode Sector of Usual Address
Organisation Code (PCT of Residence)
Patient Postcode Electoral Ward
Area Code Derived
Organisation Code Type PCT of Residence
SHA Type from Patient Postcode
Census Output Area 2001
Country
County Code
ED County Code
ED District Code
Electoral Ward Division
Government Office Region Code
Local Authority Code
SHA Old Org Code
Electoral Ward 1998
Attendance Identifier
Administrative Category
Attended Or Did Not Attend
First Attendance
Outcome Of Attendance
Medical Staff Type Seeing Patient
Source of Referral for Outpatients
Appointment Date
Operation Status
OP Episode Type
CDS Activity Date
Attendance Date
Attender Type Derived
Commissioning Serial No (Agreement No)
NHS Service Agreement Line No

Provider Reference No
Commissioner Reference No
SHA Commissioner
SHA Provider
Organisation Code (Code of Provider)
Provider Site Code
Organisation Code (Code of Commissioner)
Commissioner Code (Original Data)
Commissioner Site Code
PCT Derived from GP
PCT Derived from GP Practice
GP Practice Derived from PDS
Location Class
Site code of Treatment
Organisation Code Type Provider
Organisation Code Type Commissioner
GP PCT Type (Derived)
PCT of Residence (Original)
PCT Responsible
Location Type Code
Attendance Organisation Code Type
Provider Location
Consultant Code
Main Specialty Code
Treatment Function Code
Consultant Code Type
Consultant Organisation Code
Organisation Code Type Consultant
Registered GMP Code
GP Code
GP Practice Code
GP Consortium Code
GP Practice Code (Original Data)
GP Practice Code (Derived)
Referrer Code
Referring Organisation Code
GP Code Type
Organisation Code Type GP
First GP Organisation Code
Organisation Code of GP
SHA from GP (Derived)
SHA Type from GP (Derived)
Referrer Code Type
Organisation Code Type Referrer
Priority Type
Service Type Requested
Referral Request Received Date
Last DNA or Patient Cancelled Date
Request Received Date Status
Last Did Not Arrive Date
Spell Version As At Date And Time
Applicable Costing Period
PbR Spell Status Indicator
PbR Spell Frozen Indicator
PbR Spell Cost ID
Spell Cost Version Date
Spell Error Status
Spell Const Version No
HRG (Submitted)
Core HRG Version (Calculated)
Core HRG
SUS HRG
HRG Version (Submitted)
HRG Dominant Grouping Variable

Procedure
Unbundled HRG 1
Unbundled HRG 2
Unbundled HRG 3
Unbundled HRG 4
Unbundled HRG 5
Unbundled HRG 6
Unbundled HRG 7
Unbundled HRG 8
Unbundled HRG 9
Unbundled HRG 10
Unbundled HRG 11
Unbundled HRG 12
HRG Dominant Grouping Variable
HRG Procedure Scheme
Diagnosis Scheme In Use
Primary Diagnosis Code
Secondary Diagnosis Code 1
Secondary Diagnosis Code 2
Secondary Diagnosis Code 3
Secondary Diagnosis Code 4
Secondary Diagnosis Code 5
Secondary Diagnosis Code 6
Secondary Diagnosis Code 7
Secondary Diagnosis Code 8
Secondary Diagnosis Code 9
Secondary Diagnosis Code 10
Secondary Diagnosis Code 11
Secondary Diagnosis Code 12
Procedure Scheme In Use
Primary Procedure Code
Secondary Procedure Code 1
Secondary Procedure Date 1
Secondary Procedure Code 2
Secondary Procedure Date 2
Secondary Procedure Code 3
Secondary Procedure Date 3
Secondary Procedure Code 4
Secondary Procedure Date 4
Secondary Procedure Code 5
Secondary Procedure Date 5
Secondary Procedure Code 6
Secondary Procedure Date 6
Secondary Procedure Code 7
Secondary Procedure Date 7
Secondary Procedure Code 8
Secondary Procedure Date 8
Secondary Procedure Code 9
Secondary Procedure Date 9
Secondary Procedure Code 10
Secondary Procedure Date 10
Secondary Procedure Code 11
Secondary Procedure Date 11
Secondary Procedure Code 12
Secondary Procedure Date 12
Primary Procedure Date
HRG Used for Tariff
Tariff Initial Amount National
Aggregate UnBundled Adjustment National
Tariff Financial Adjustment National
Tariff Adjustment Future Use_1 National
Tariff Adjustment Future Use_2 National
Tariff Pre MFF Adjusted National
Applied MFF National

MFF Adjustment
Tariff Total Payment National
Outpatient Tariff
Market Forces Factor ID
Tariff Initial Amount Non Mandatory
Aggregate UnBundled Adjustment Non Mandatory
Tariff Financial Adjustment Non Mandatory
Tariff Adjustment Future Use_1 Non Mandatory
Tariff Adjustment Future Use_2 Non Mandatory
Tariff Pre MFF Adjusted Non Mandatory
Applied MFF Non Mandatory
MFF Adjustment Non Mandatory
Tariff Total Payment Non Mandatory
Non Mandatory Core Tariff (with UB)
Tarrif Initial Amount Local
Aggregate UnBundled Adjustment Local
Tariff Total Payment Local
Local Core Tariff (with UB)
PbR Final Tariff
Final Tariff Applied
Number Diagnosis
Number Procedures
Number Unbundled HRGs
Number Unbundled Non Priced HRGs
Number Unbundled Priced HRGs
Number BPT Indicators
Organisation Code (Sender)
Staging Loaded Date
Protocol Identifier
Unique CDS Identifier
Applicable Date
Extract Date
Report Period Start Date
Report Period End Date
Organisation Code Type Sender
Match Criterion Indicator
Costing Batch Sequence
Current Period Number
Finished Indicator
HES Identifier
Intended Procedure Status
Interchange ID
Prime Recipient
Organisation Code Type Prime Recipient
Other Indicator
PbR Generated Interchange ID
Record Extraction Indicator
Re-costing Requested Flag
Temporary Cost Period Status
Test Indicator
Update Type
Version Sequence Number
Hierarchy
Costed Indicator
Spare 1
Spare 2
Spare 3
Spare 4
Spare 5
Direct access tariff flag
Spell NPOC

Spell Service Line
Commissioning Region
Unbundled exclusion reason
Grouping Algorithm Version
Grouping Reference Data Version
Grouping HRG Version
CDS Schema Version
Query Date
Unique Query Id
Copy Recipients
Derived Commissioner
Derived Commissioner Type
Is Valid UBRN
UBRN Occurrence Count

Accident and Emergency (A&E) Admission Fields

SUS Version
NHS RID (From Provider)
CDS Record Type
Reason Access Provided
CDS Group Derived
CDS Group Indicator
Bulk Replacement CDS Group
Spell In PbR/Not In PbR
Exclusion Reason
Pseudonymised Status
Confidentiality Category
Configurable Indicator
Code Cleaning
NHS Number
Lead Care Activity Indicator
Organisation Code Patient Pathway Identifier
RTT Patient Pathway Identifier
RTT Period End Date
RTT Period Start Date
RTT Status
Unique Booking Reference Number (Converted)
RTT Length (Derived)
Age At CDS Activity Date
Derived Age
Patient Type
Age Range Derived
Year of Birth
Month of Birth
Age at Record Start
Age at Record End
Carer Support Indicator
Ethnic Category Code
Marital Status
NHS Number Status Indicator
Gender Code
Postcode Sector of Usual Address
Organisation Code (PCT of Residence)
Patient Postcode Electoral Ward
SHA Type from Patient Postcode
Area Code Derived
Organisation Code Type PCT of Residence
PCT of Residence (Original)
PCT Responsible
Census Output Area 2001
Country
County Code
ED County Code
ED District Code
Electoral Ward Division
Government Office Region Code
Local Authority Code
SHA Old Org Code
Electoral Ward 1998
EM Attendance Number
EM Mode of Arrival
EM Attendance Category
EM Attendance Disposal
EM Incident Location Type
EM Staff Member Code
EM Referral Source
Arrival Date
EM Patient Group
EM Attendance Conclusion Time
EM Departure Time
EM Initial Assessment Time
EM Time Seen for Treatment
Arrival Time
CDS Activity Date
EM Attendance Category ID
Consultant Code Type
Consultant Organisation Code
Organisation Code Type Consultant
EM Conclusion Waiting Time
EM Duration Time
EM Assessment Waiting Time
EM Treatment Wait Time
Commissioning Serial No (Agreement No)
NHS Service Agreement Line No
Provider Reference No
Commissioner Reference No
SHA Commissioner
SHA Provider
Organisation Code (Code of Provider)
Provider Site Code
Organisation Code (Code of Commissioner)
Commissioner Code (Original Data)
Commissioner Site Code
PCT Derived from GP
PCT Derived from GP Practice
GP Practice Derived from PDS
Organisation Code Type Provider
Provider Code (Original Data)
Organisation Code Type Commissioner
GP PCT Type (Derived)
Registered GMP Code
Registered GMP Code (Original Data)
GP Practice Code (Original Data)
GP Practice Code
GP Consortium Code
GP Code Type
Organisation Code GP
Organisation Code Type GP
First GP Organisation Code
SHA from GP (Derived)
SHA Type from GP (Derived)
Spell Version As At Date And Time
Applicable Costing Period
PbR Spell Status Indicator
PbR Spell Frozen Indicator
HRG Code - Submitted
HRG Code Version - Submitted
Core HRG
HRG Code Version - Calculated
HRG Dominant Grouping Variable
HRG Dominant Grouping Variable Procedure
HRG Procedure Scheme
Diagnosis Scheme In Use
ICD 10 Primary Diagnosis
Secondary Diagnosis Code 1
Secondary Diagnosis Code 2
Secondary Diagnosis Code 3
Secondary Diagnosis Code 4
Secondary Diagnosis Code 5
Secondary Diagnosis Code 6
Secondary Diagnosis Code 7
Secondary Diagnosis Code 8
Secondary Diagnosis Code 9
Secondary Diagnosis Code 10
Secondary Diagnosis Code 11
Secondary Diagnosis Code 12
EM Diagnosis First
EM Diagnosis Second 1
EM Diagnosis Second 2
EM Diagnosis Second 3
EM Diagnosis Second 4
EM Diagnosis Second 5
EM Diagnosis Second 6
EM Diagnosis Second 7
EM Diagnosis Second 8
EM Diagnosis Second 9
EM Diagnosis Second 10
EM Diagnosis Second 11
EM Diagnosis Second 12
Diagnosis Type
Investigation Scheme In Use
EM Investigation First
EM Investigation Second 1
EM Investigation Second 2
EM Investigation Second 3
EM Investigation Second 4
EM Investigation Second 5
EM Investigation Second 6
EM Investigation Second 7
EM Investigation Second 8
EM Investigation Second 9
EM Investigation Second 10
EM Investigation Second 11
EM Investigation Second 12
Procedure Scheme In Use
EM Treatment First
PROCEDURE DATE (of First Treatment)
EM Treatment Second 1
PROCEDURE DATE (of Subsequent Treatments) 1
EM Treatment Second 2
PROCEDURE DATE (of Subsequent Treatments) 2
EM Treatment Second 3
PROCEDURE DATE (of Subsequent Treatments) 3
EM Treatment Second 4
PROCEDURE DATE (of Subsequent Treatments) 4
EM Treatment Second 5
PROCEDURE DATE (of Subsequent Treatments) 5
EM Treatment Second 6
PROCEDURE DATE (of Subsequent Treatments) 6
EM Treatment Second 7
PROCEDURE DATE (of Subsequent Treatments) 7
EM Treatment Second 8
PROCEDURE DATE (of Subsequent Treatments) 8
EM Treatment Second 9
PROCEDURE DATE (of Subsequent Treatments) 9
EM Treatment Second 10
PROCEDURE DATE (of Subsequent Treatments) 10
EM Treatment Second 11
PROCEDURE DATE (of Subsequent Treatments) 11
EM Treatment Second 12
PROCEDURE DATE (of Subsequent Treatments) 12
PRIMARY PROCEDURE
Primary Procedure Date
Secondary Procedure Code 1
Secondary Procedure Date 1
Secondary Procedure Code 2
Secondary Procedure Date 2
Secondary Procedure Code 3
Secondary Procedure Date 3
Secondary Procedure Code 4
Secondary Procedure Date 4
Secondary Procedure Code 5
Secondary Procedure Date 5
Secondary Procedure Code 6
Secondary Procedure Date 6
Secondary Procedure Code 7
Secondary Procedure Date 7
Secondary Procedure Code 8
Secondary Procedure Date 8
Secondary Procedure Code 9
Secondary Procedure Date 9
Secondary Procedure Code 10
Secondary Procedure Date 10
Secondary Procedure Code 11
Secondary Procedure Date 11
Secondary Procedure Code 12
Secondary Procedure Date 12
Derived EM Department Type
EM Department Type
EM Department Type MIU Indicator Derived
Tariff Initial Amount National
Tariff Financial Adjustment National
Tariff Adjustment Future Use_1 National
Tariff Adjustment Future Use_2 National
Tariff Pre MFF Adjusted National
Applied MFF National
MFF Adjustment
Tariff Total Payment National
EM Tariff ID
Market Forces Factor ID
Tariff Initial Amount Non Mandatory
Tariff Financial Adjustment Non Mandatory
Tariff Adjustment Future Use_1 Non Mandatory
Tariff Adjustment Future Use_2 Non Mandatory
Tariff Pre MFF Adjusted Non Mandatory
Applied MFF Non Mandatory
MFF Adjustment Non Mandatory
Tariff Total Payment Non Mandatory
Tarrif Initial Amount Local
Tariff Total Payment Local
PbR Final Tariff
Final Tariff Applied
Number Diagnosis
Number Procedures
Number EM Investigations
Number EM Treatments
Organisation Code (Sender)
Staging Loaded Date
Protocol Identifier
Unique CDS Identifier
Applicable Date and Time
Extract Date
Report Period Start Date
Report Period End Date
Organisation Code Type Sender
Match Criterion Indicator
Cost Period Spell Status Indicator
Costed Indicator
Costing Batch Sequence
Current Period Number
Finished Indicator
HES Identifier
Intended Procedure Status
Interchange ID
Attendance Location Class
Location Type Code
Attendance Site Code
Prime Recipient
Organisation Code Type Prime Recipient
Organisation Code Type Location
Other Indicator
PbR Generated Interchange ID
Spell Const Version No
PbR Spell Cost ID
PbR Spell Cost Version Date
Provider Location
Record Extraction Indicator
Re-costing Requested Flag
Referrer Code Type
Organisation Code Type Referrer
First Referrer Organisation Code
Spell Complete Indicator
Temporary Cost Period Status
Test Indicator
Update Type
Version Sequence Number
Maximum Episode Date
Hierarchy
PbR Spell Service ID Version
Spell Error Status
Spare 1
Spare 2
Spare 3
Spare 4
Spare 5
Grouping Algorithm Version
Grouping Reference Data Version
Grouping HRG Version
CDS Schema Version
Query Date
Unique Query Id
Copy Recipients
Derived Commissioner
Derived Commissioner Type

Risk Assessment

SOURCES

Data Protection Act 2018 (DPA)

General Data Protection Regulations (EU) 2016/679 (GDPR)

Information Commissioner – Guide to the General Data Protection Regulations (ICO Guide)

Information Commissioner - Data Protection Impact Assessments

1. INTRODUCTION

The UK Information Commissioner and the European Data Protection Board provide that Data Protection Impact Assessments are necessary, in certain circumstances, to assess the level of risk to the rights and freedoms of individuals.

Controllers must consider both the likelihood and the severity of any impact on individuals. High risk could result from either a high probability of some harm, or a lower possibility of serious harm.

The risk assessment serves to support Controller customers to identify the level of inherent risk so that the measures being put in place to mitigate the risk are proportionate to the impact that projects or initiatives might have on data subjects.

2. ACCOUNTABILITY

Prescribing Services Ltd (PSL) are a Processor and are therefore required to provide assurance that their technical and organisational measures that are comparable to those implemented by the Controller and proportionate to the risk.

Unlike the Controller, they are not in a position to assess the risk to the rights and freedoms of particular data subjects since they are not in control of establishing the lawful basis or a direct route for giving effect to data subject rights. However, due to the nature and scope of processing, it seems reasonable to assume that implementing the described project represents at least a moderate to high degree of risk to the rights and freedoms of data subjects in the event that appropriate technical and organisational measures are not put in place at all. This assessment will therefore explore each of the elements drawn out within data protection legislation for mitigation of those risks.

3. ASSET CRITICALITY SCORING GRID

Typically, critical national services. Absence of system leads to complete failure of dependent systems and services with a high possibility of personal safety issues. Service interruption results in severe reputational damage	5
Predominantly transactional services. Absence leads to operational difficulties that can be coped with for a limited period. May lead to increased risk to stakeholders or organisation.	4
Predominantly data capture, batch processing. Absence leads to operational difficulties, but these are manageable for an extended 2period. Eg. 1 day. Absence of system may lead to a slight increase in risk to stakeholders or organisation.	3
Business Hours Support (8am-6pm) Mon-Fri (not BH). Service Availability 98%. DR optional - dependant on outcome of BIA.	2

4. DATA RISK SCORING GRID

Data is aggregated and anonymised.	2
Low volume of personal data involved or high volumes of anonymised data.	3
High-volume personal data or low volume special category data.	4
High volume and special category data or includes stigmatised information (i.e. mental health data).	5

5. RISK SCORING MATRIX

		Asset Criticality			
		2	3	4	5
Impact of data breach	2	🟧 Bronze	🟧	⬜	🟨
	3	🟧	⬜ Silver	🟨	🟨
	4	⬜	🟨	🟨 Gold	⬛
	5	🟨	🟨	⬛	⬛ Platinum

6. ASSESSMENT AND RATIONALE

What score has the project been given in terms of criticality of resulting asset or service?	Predominantly transactional services. Absence leads to operational difficulties that can be coped with for a limited period. May lead to increased risk to clinical care.
Rationale	Whilst the systems and services provided by PSL are ordinarily supplementary to core clinical services, they are increasingly being used to identify cohorts of patients who require specific interventions in relation to cancer pathways, for example, or as a result of the pandemic. To reflect that, this assessment has heightened the potential critically based on the fact that some customers may rely more on the services that others. By assessing the service in this way, it allows the design and underlying

	compliance to reflect a potential future state whereby PSL services are fundamental to supporting core health and care services.
What score has the project been given in terms of the nature and volume of data being processed?	High volume and special category data and includes stigmatised information.
Rationale	PSL are supporting many GPs and CCG across the country which results in thousands of patients' data being extracted on a daily basis. This includes read coded, de-identified data that this includes health information - including stigmatised information. Whilst the data is de-identified, this assessment takes the approach of assuming highest risk such that customers are assured with regards to measures adopted to reduce risk.
Overall risk score given to the processing activity / project in question.	GOLD
Does the project involve introduction of a cloud service to be assessed?	Introduces cloud services that will need to be assessed

6. RISK ASSESSMENT CONCLUSION

The project has been assessed to have an overall risk score of GOLD and so the measures to be applied will be proportionate to reduce the inherent risk levels to a suitable level such that they can be accepted by the Controller.

Controllers and Processors

SOURCES

Data Protection Act 2018 (DPA)

General Data Protection Regulations (EU) 2016/679 (GDPR)

Information Commissioner – Guide to the General Data Protection Regulations (ICO Guide)

ICO Guidance - Data Controllers

KAFICO

INFORMATION · GOVERNANCE · CONSULTANCY

1. DEFINITIONS / CONTEXT

“It is essential for organisations involved in the processing of personal data to be able to determine whether they are acting as a data controller or as a data processor in respect of the processing. This is particularly important in situations such as a data breach where it will be necessary to determine which organisation has data protection responsibility.

The data controller must exercise overall control over the purpose for which, and the manner in which, personal data are processed. However, in reality a data processor can itself exercise some control over the manner of processing – e.g. over the technical aspects of how a particular service is delivered.

The fact that one organisation provides a service to another organisation does not necessarily mean that it is acting as a data processor. It could be a data controller in its own right, depending on the degree of control it exercises over the processing operation.”[1]

2. DATA CONTROLLERS

GP Practices has been assessed to be a Data Controller.

This is because;

- They decided to collect or process the personal data.
- They decided what the purpose or outcome of the processing was to be.
- They decided what personal data should be collected.
- They decided which individuals to collect personal data about.

[1] https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf

- They make decisions about the individuals concerned as part of or as a result of the processing.
- They exercise professional judgement in the processing of the personal data.
- They have a direct relationship with the data subjects.
- They have complete autonomy as to how the personal data is processed.
- They have appointed the processors to process the personal data on their behalf.

Clinical Commissioning Groups have also been assessed to be a Data Controller.

This is because;

- They decided to collect or process the personal data.
- They decided what the purpose or outcome of the processing was to be.
- They decided what personal data should be collected.
- They decided which individuals to collect personal data about.
- They make decisions about the individuals concerned as part of or as a result of the processing.
- They exercise professional judgement in the processing of the personal data.
- They have appointed the processors to process the personal data on their behalf

2. DATA PROCESSORS

Prescribing Services Limited has been assessed to be a Data Processor.

This is because;

- They are following instructions from someone else regarding the processing of personal data.

- They were given the personal data by a customer or similar third party, or told what data to collect.
- They do not decide to collect personal data from individuals.
- They do not decide what personal data should be collected from individuals.
- They do not decide the lawful basis for the use of that data.
- They do not decide what purpose or purposes the data will be used for.
- They do not decide whether to disclose the data, or to whom.
- They do not decide how long to retain the data.
- They may make some decisions on how data is processed, but implement these decisions under a contract with someone else.
- They are not interested in the end result of the processing.

Wellbeing Software (Apollo) has been assessed to be a Sub Processor.

This is because;

- They are following instructions from someone else regarding the processing of personal data.
- They were given the personal data by a customer or similar third party or told what data to collect.
- They do not decide to collect personal data from individuals.
- They do not decide what personal data should be collected from individuals.
- They do not decide the lawful basis for the use of that data.
- They do not decide what purpose or purposes the data will be used for.
- They do not decide whether to disclose the data, or to whom.
- They do not decide how long to retain the data.
- They may make some decisions on how data is processed, but implement these decisions under a contract with someone else.
- They are not interested in the end result of the processing.

The Bunker has also been assessed to be a Sub Processor.

This is because;

- They are following instructions from someone else regarding the processing of personal data.
- They were given the personal data by a customer or similar third party, or told what data to collect.
- They do not decide to collect personal data from individuals.
- They do not decide what personal data should be collected from individuals.
- They do not decide the lawful basis for the use of that data.
- They do not decide what purpose or purposes the data will be used for.
- They do not decide whether to disclose the data, or to whom.
- They do not decide how long to retain the data.
- They may make some decisions on how data is processed but implement these decisions under a contract with someone else.
- They are not interested in the end result of the processing.

3. APPROPRIATE SHARING DOCUMENTS

.

“It is good practice for you to have written data sharing agreements when controllers share personal data. This helps everyone to understand the purpose for the sharing, what will happen at each stage and what responsibilities they have. It also helps you to demonstrate compliance in a clear and formal way. Similarly, written contracts help controllers and processors to demonstrate compliance and understand their obligations, responsibilities and liabilities."2

The stakeholders have the following in place;

- A Processing Contract between GP Practices and PSL
- A Processing Contract between PSL and CCG
- A Processing Contract between PSL and Apollo
- A Processing Contract between PSL and The Bunker

The CCG and the GP Practices will also have between them;

- A Data Sharing Agreement approved by NHS Digital that names PSL as an approved Risk Stratification provider

PROCESSING CONTRACT REVIEWS

In accordance with s 56 of the Data Protection Act 2018, there is a need to ensure that the legally required processing clauses are included in any contract between a Controller and Processor or Processor and Sub Processors.

Name of Supplier: PSL

Contract reviewed: PSL GP Processing Contract

Clause	Status	Comments
Is the processor required to provide, on request evidence that they have implemented appropriate technical and organisational measures to protect Personal Data including storage and transmission of data, business continuity, staff training, auditing, access control and Cyber security?	Yes	Section 2.9.5

[2] https://ico.org.uk/for-organisations/accountability-framework/contracts-and-data-sharing/

Does the contract state that the processor shall not engage another processor without prior specific or general written authorisation of the controller?	Yes	2.5
Does the contract set out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller?	Yes	Schedule 1
Does the contract stipulate that the Processor processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by law and in those cases will notify the Controller?	Yes	2.9.4
Does the contract state that all staff employed by the processor have contracts that include confidentiality clauses and that Personal Data will not be shared with third party unless required to do so by law?	Yes	Yes
Does the contract require the Processor to assist the Controller to respond to requests for exercising the data subject's rights i.e. access to information, correction of errors?	Yes	2.9.7
Does the contract require the Processor to assist the Controller in reporting information incidents promptly including where it might be required to contact the data subject?	Yes	2.9.7
Does the contract state what should happen to the data at the end of the contract or in the event of termination such as return of the data or secure destruction?	Yes	Schedule 2
Does the contract require the Processor to allow for a comply with audits including inspections conducted by the Controller or a third party engaged by the Controller?	Yes	2.10

Name of Supplier: Wellbeing Software

Contract reviewed: Apollo Services Agreement

Clause	Status	Comments
Is the processor required to provide, on request evidence that they have implemented appropriate technical and organisational measures to protect Personal Data including storage and transmission of data, business continuity, staff training, auditing, access control and Cyber security?	Yes	s 4.10.2 (c)
Does the contract state that the processor shall not engage another processor without prior specific or general written authorisation of the controller?	Yes	4.2.10 (e)
Does the contract set out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller?	Yes	Specified in the customer Project Order (separate)
Does the contract stipulate that the Processor processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by law and in those cases will notify the Controller?	Yes	s 5.8.2
Does the contract state that all staff employed by the processor have contracts that include confidentiality clauses and that Personal Data will not be shared with third party unless required to do so by law?	Yes	Yes
Does the contract require the Processor to assist the Controller to respond to requests for exercising the	Yes	4.2.10 (i)

data subject's rights i.e. access to information, correction of errors?		
Does the contract require the Processor to assist the Controller in reporting information incidents promptly including where it might be required to contact the data subject?	Yes	4.2.10 (m)
Does the contract state what should happen to the data at the end of the contract or in the event of termination such as return of the data or secure destruction?	Yes	6.3
Does the contract require the Processor to allow for a comply with audits including inspections conducted by the Controller or a third party engaged by the Controller?	Yes	4.2.10 (j)

Name of Supplier: The Bunker

Contract reviewed: The Bunker GDPR Addendum

Clause	Status	Comments
Is the processor required to provide, on request evidence that they have implemented appropriate technical and organisational measures to protect Personal Data including storage and transmission of data, business continuity, staff training, auditing, access control and Cyber security?	Yes	s 2.5.2
Does the contract state that the processor shall not engage another processor without prior specific or general written authorisation of the controller?	Yes	s 2.6
Does the contract set out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and	Yes	Data Processor Addendum

categories of data subjects and the obligations and rights of the controller?		
Does the contract stipulate that the Processor processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by law and in those cases will notify the Controller?	Yes	s 2.5.1
Does the contract state that all staff employed by the processor have contracts that include confidentiality clauses and that Personal Data will not be shared with third party unless required to do so by law?	Yes	Yes
Does the contract require the Processor to assist the Controller to respond to requests for exercising the data subject's rights i.e. access to information, correction of errors?	Yes	2.5.5
Does the contract require the Processor to assist the Controller in reporting information incidents promptly including where it might be required to contact the data subject?	Yes	s 2.5.5
Does the contract state what should happen to the data at the end of the contract or in the event of termination such as return of the data or secure destruction?	Yes	s 2.5.7
Does the contract require the Processor to allow for a comply with audits including inspections conducted by the Controller or a third party engaged by the Controller?	Yes	s 2.5.8

Lawful Processing

SOURCES

Data Protection Act 2018 (DPA)

General Data Protection Regulations (EU) 2016/679 (GDPR)

Information Commissioner – Guide to the General Data Protection Regulations (ICO Guide)

The Health and Social Care (Safety and Quality) Act 2015: Duty to share information (HSCA)

KAFICO

INFORMATION · GOVERNANCE · CONSULTANCY

1. DEFINITIONS / CONTEXT

Controllers must have a valid lawful basis in order to process personal data.

There are six available lawful bases for processing. No single basis is ’better’ or more important than the others – which basis is most appropriate to use will depend on your purpose and relationship with the individual.

Most lawful bases require that processing is ‘necessary’. If Controllers can reasonably achieve the same purpose without the processing, they won’t have a lawful basis.

Controllers must determine the lawful basis before they begin processing, and should document it.

Controller’s privacy notices should include your lawful basis for processing as well as the purposes of the processing.

If the purposes change, Controllers may be able to continue processing under the original lawful basis if the new purpose is compatible with the initial purpose (unless the original lawful basis was consent).

If Controllers are processing special category data they will need to identify both a lawful basis for general processing and an additional condition for processing this type of data.

The conditions for CCGs undertaking automated processing such as risk stratification may also be “public task” and “medical purposes”

Where such processing could result in a decision that affects an individual, must offer a right to object before such decisions are taken, in accordance with Article 22.

Where CCGs are collecting data as part of a legal requirement, for example where NHS Digital is directed to collect specified data via CCG, lawful basis is “compliance with a legal obligation”

2. DATA CATEGORIES

The UK GDPR / DPA 18 and EU GDPR governs the processing of data that identifies living individuals and provides that Special Categories of Data is personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, data concerning health or data concerning a natural person’s sex life or sexual orientation.

The initiative involves processing of Personal Data and Special Category Data and therefore requires both a lawful basis under Art 6 UK GDPR and an condition for processing of Special Category Data

Data Processors are not in a position to determine the purpose and means of processing. However, for the purposes of supporting customers with their assessments, the following assumptions have been made.

3. LAWFUL BASIS FOR PROCESSING PERSONAL DATA

UK GDPR Article 6 (e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

4. CONDITION FOR PROCESSING SPECIAL CATEGORY DATA

Article 9 2 (h) Health or social care (with a basis in law)

5. OBLIGATIONS OF SECRECY

Both Data Protection Act 2018 and GDPR indicate that healthcare data may be processed by healthcare providers - where the law makes provision for such services (i.e. registered healthcare professionals) or by a third party “pursuant to a contract” that creates an obligation of secrecy or “a person who in the circumstances owes a duty of confidentiality”.

Controllers are permitted to delegate their processing functions to another organisation, who collect, store, retain, display, link and destroy the data on their behalf as Processors.

There is a Processing Contract in place with the Processor to ensure that they are bound to secrecy.

6. NECESSITY

As previously identified, the Controller has responsibility to ascertaining lawful basis however, the following presumptions are made.

The processing is ***necessary*** for healthcare purposes because there is a statutory duty under HSCA for healthcare providers to;

Share information between health or adult social care commissioners or providers

This project will involve sharing information between health and social care commissioners and providers

Where lawful and the individual has not objected

Any existing objections to data being processed will be observed by virtue of excluding patients that have “opted out” from the extracted data set.

For the purposes likely to facilitate the provision of health services or adults social care

The sharing will provide information that supports consultations, emergency care, diagnosis directly to the individual patient and broader healthcare management.

Where it is in the individual’s best interest.

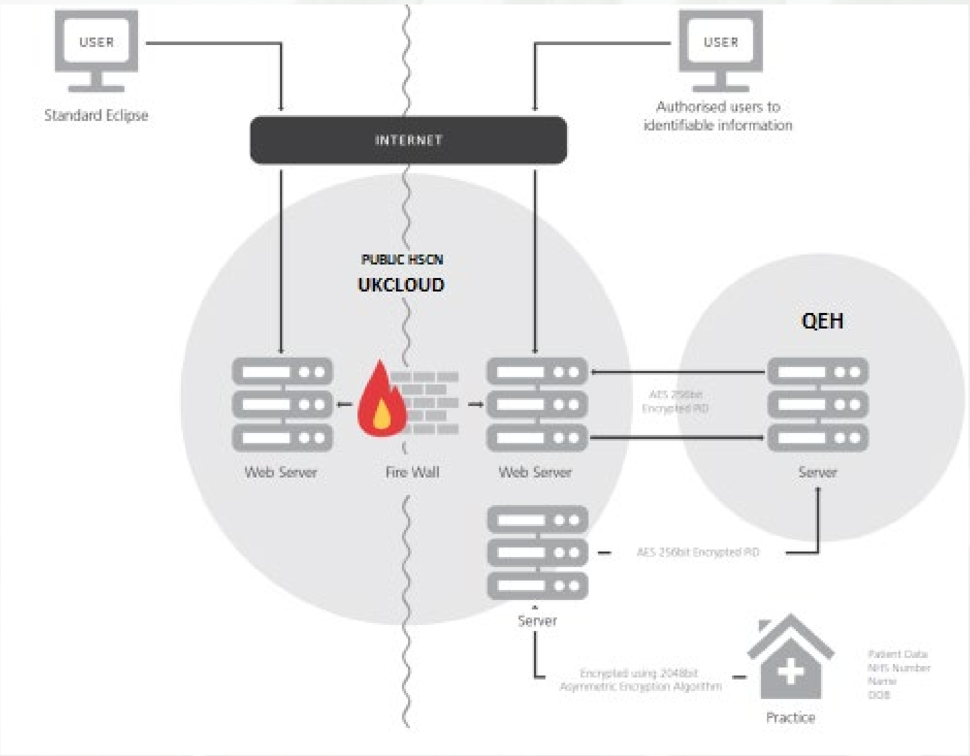
Improved and informed patient care is at the heart of the project.

7. EXPECTATIONS / COMMON LAW CONFIDENTIALITY

Section 251 CAG7-04(a)/2013 of the NHS Act 2006 and the Regulations enable the common law duty of confidentiality to be temporarily lifted so that confidential patient information can be transferred to an applicant without the discloser being in breach of the common law duty of confidentiality..

8. DE-IDENTIFICATION / PSEUDONYMISATION

Advice and Guidance (Eclipse Live) employs pseudonymisation to protect data both in transit and at rest. This is demonstrated below;



Recital 26, the GDPR limits the ability of a data handler to benefit from pseudonymized data if re-identification techniques are “reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly.”

To determine how effectively the linked data has been pseudonymised (and therefore further minimised where a large and somewhat speculative data set exists), it is necessary to consider how “reasonably likely” it is that the Controller (or Processor) or another person could directly or indirectly identify a person.

This should consider the time, cost and effort necessary to do so.

The data being held at the QEH Server is;

- Eclipse No (clear)
- Name (encrypted)
- Address (encrypted)
- NHS No (encrypted)
- DOB (encrypted)

All the other data is 256-bit encrypted and they key for which is only available on another server which is hosted by PSL at their own location.

The data held at PSL servers is the linked, pooled data set ***without***;

- Name (encrypted)
- Address (encrypted)
- NHS No (encrypted)
- DOB (encrypted)

And ***with*** the Eclipse Identifier.

This information is also 256-bit encrypted but the decryption key for this information is within the same location and available to a limited number of individuals.

Practice data set extracted manually or by Wellbeing Software (Apollo);

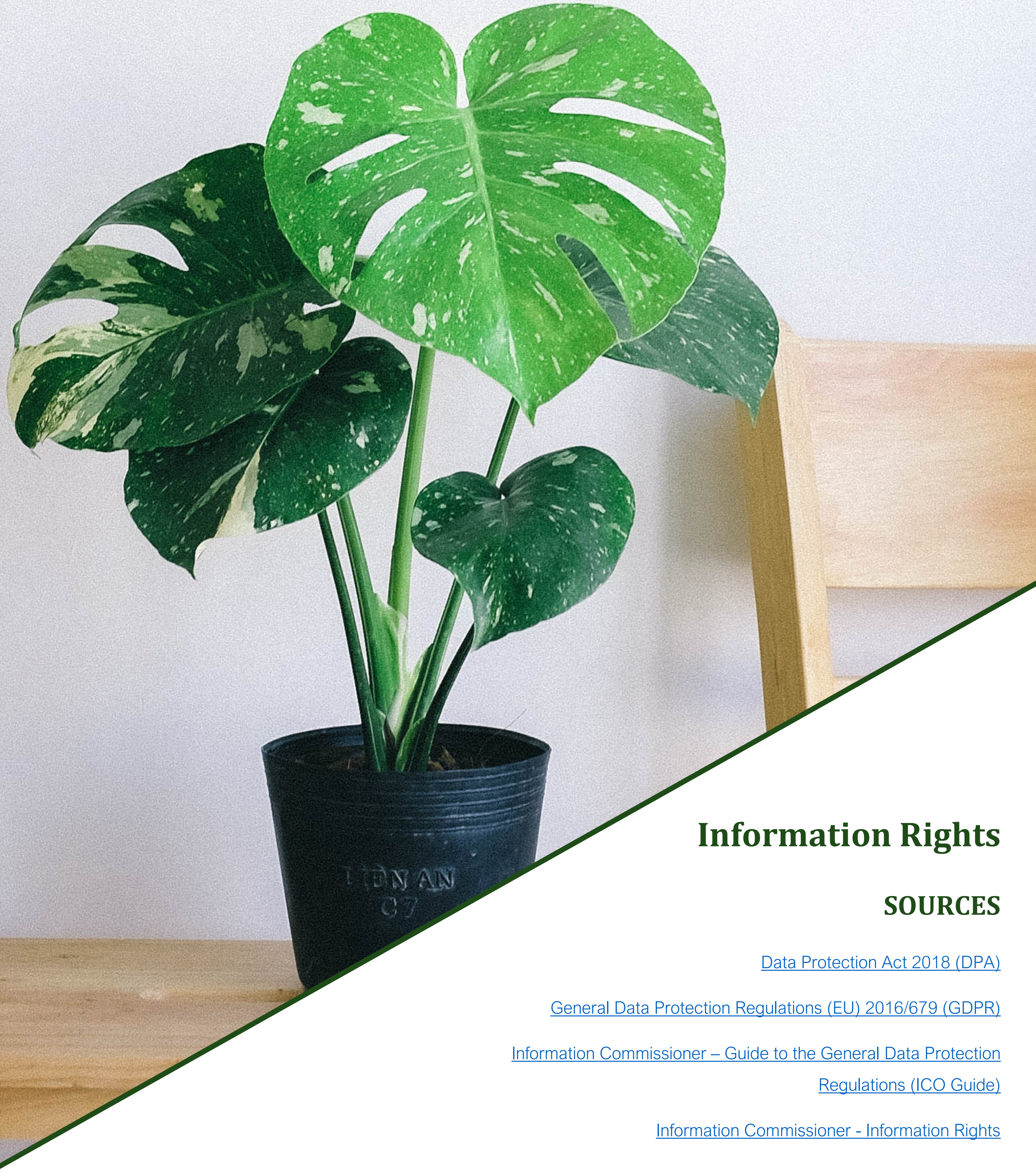
- Demographics

- age (years)
- gender
- clinical system no
- Coded event data
- Clinical sys no
- Read Code (Value 1 value 2)
- Medication data
- medication name
- medication read codes
- Date issued
- status (repeat etc)
- Instructions - free text)

The data is 256-bit encrypted which is regarded as requiring significant cost, time and effort in order to decrypt without the necessary key.

It is also worth noting that the data is read coded which provides another layer of protection should the information be inappropriately disclosed.

It is therefore determined that, due to the de-identification, creation of a unique integer, encryption and location of the data across multiple locations, the risk of reidentification of the data sets by a motivated intruder is low.



Information Rights

SOURCES

Data Protection Act 2018 (DPA)

General Data Protection Regulations (EU) 2016/679 (GDPR)

Information Commissioner – Guide to the General Data Protection Regulations (ICO Guide)

Information Commissioner - Information Rights

KAFICO

INFORMATION · GOVERNANCE · CONSULTANCY

1. DEFINITIONS / CONTEXT

The UK and EU GDPR provides the following rights for individuals: The right to be informed, the right of access, the right to rectification, the right to erasure, the right to restrict processing, the right to data portability, the right to object, rights in relation to automated decision making and profiling.

Processors are contractually bound to supporting Customer Controllers with their information rights requests by virtue of Data Processing Contract. This means that they will work to support the Controller towards a timely and complete response to any request made by data subjects.

2. FACILITATION OF INFORMATION RIGHTS

Information Right	Applies?	How Supported
Right to Access	Yes, data subjects do have a right to request access to their information under this lawful basis.	The PSL systems and architecture allows personal data to be extracted / printed and provided to data subject on request. End users can view, add notes to an alert, or an action plan connected to a priority patient. All this activity is retained within the system and can be retrieved for the purposes of providing copies to data subjects. The system provides an audit trail of extractions and reports such that these can also form part of a subject access request response as well.
Rectification and Restriction	Yes, data subjects do have a right to request the rectification	The PSL systems and architecture allows personal data to be amended / access restricted and provides an audit trail of such amendments.

	and restriction of their personal data under this lawful basis.	Since patients largely do not have a direct relationship with PSL and PSL would be unable to identify a particular individual, it is anticipated that these rights would be actioned by the healthcare provider at source. Where an Eclipse user identifies an inaccuracy at source and adds a read code or alters basic demographics, this will automatically be included in the Eclipse data extraction. For example, the GP adds a new allergy to the record because the patient has flagged it. The next extraction performed by Eclipse will include that information and this will be available to other users.
Portability	The right to data portability only applies when your lawful basis for processing this information is consent or for the performance of a contract and so would not apply to processing under this DPIA.	Not Applicable
Erasure	The right to Erasure does not apply when processing is for Public Task and Medical Purposes and so would not apply to processing under this DPIA.	Not Applicable
Object	Yes, the data subject does have a right to object to processing of their personal data under this lawful basis.	The data subjects' ability to raise objections via the Controller is unaffected by this project. The extractions already exclude patients that have exercised objections via the NHS National Data Opt Out programme.

3. PROFILING AND AUTOMATED DECISION MAKING

Data Protection Law has provisions on:

- automated individual decision-making (making decisions solely by automated means without any human involvement) and;
- profiling (automated processing of personal data to evaluate certain things about an individual). Profiling can be part of an automated decision-making process.

Article 22 protects individuals if you are carrying out solely automated decision-making that has legal or similarly significant effects on them;

Where automated decisions are made, the Controller must give individuals information about the processing; introduce simple ways for them to request human intervention or challenge a decision; carry out regular checks to make sure that your systems are working as intended.

Profiling is: Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects about the person including concerning health.

Patients have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them.

A legal effect is something that adversely affects someone's legal rights. Similarly, significant effects are more difficult to define but would include, for example, automatic refusal of an online credit application, and e-recruiting practices without human intervention.

Article 22 applies to solely automated individual decision-making, including profiling, with legal or similarly significant effects.

If your processing does not match this definition, then you can continue to carry out profiling and automated decision-making.

DETERMINATION

PSL products and services create an aggregated version of data, pulled from the Controller systems and stored by Prescribing Services and then presented to the Controller customer for use. This effectively sorts patients into particular categories for risk or health management purposes to allow the Controller customer to make decisions about suitable interventions or healthcare management decisions. There is clearly profiling taking place that results in a decision that will affect the care options available to the individual.

The patient, in this case, is subject to care decisions made as a result automated profiling into specific patient groups or the automated identification of risk factors.

In this case, there does not appear to be an impact on the legal rights of the individual nor any significant negative effect for those having decisions made about them. Where a clinician has identified risk and feel an intervention or care option is appropriate, the individual being profiled is likely to benefit from any decisions made. Additionally, the data subject retains choice and control about whether to take options provided to them such as referral to a third-party healthcare provider.

Since the processing does not fully match the definition, it is asserted that the Controller may proceed with processing without the additional restrictions under Article 22 and ensuring that information rights and transparency requirements are observed.

1. ACCURACY / INTEGRITY

There is a requirement for Controllers to ensure that suitable data quality measures are in place including how users will be trained or instructed to use systems appropriately, how records or electronic transactions will be validated against their source when added to another system, or as a result of direct data entry and how systems will react if transactions or transfers of data are not received properly.

The following is a description of the measures in place to ensure data quality and integrity, broadly, across PSL products and services.

Data Extraction

PSL have devised an algorithm that identifies when the extracted data set falls outside of expected parameters. Irregularities are highlighted through the presence of unexpected elements i.e. the size of the data set, number of data lines, number of drugs, blood pressure readings. Where the data has characteristics which could be deemed as outliers, the extraction would not be accepted by the system and this would trigger manually scrutiny.

Data Transfer

The extracted data is encrypted for transit, in order for the data set to effectively 'land', it must decrypt which means that it must be complete. It will only allow decryption and therefore accept the file if the file is complete. The systems have interoperability so rather than show corrupt data, the system will reject it.

Algorithm Application

The algorithm is programmed to create alerts when a combination of particular data points is in existence. For example, a patient who is on combination of certain medicines known to react with one another might trigger an alert for a medication review.

The algorithm is programmed using NHS England guidance and is subject to a quarterly clinical review within PSL to ensure that the data upon which the alerts are based remains accurate and best practice. The clinical team within PSL will also undertake periodic audits of alert numbers and other outliers to identify anomalies – for example, a sudden spike in the number of alerts being issued would trigger a closer look at the data being produced.

Additionally, there is a feedback button available to all end users of the system. This allows users of the system to identify where there might be gaps in the information or perhaps an alert has been inappropriately generated. So, PSL are in receipt of around 10,000 reviews supporting the ongoing development of the service.

Re-identification

The system involves a brand-new build of the integrated data sets each week. Each build requires the extraction of the data, the replacement of the identifier with the Eclipse integer.

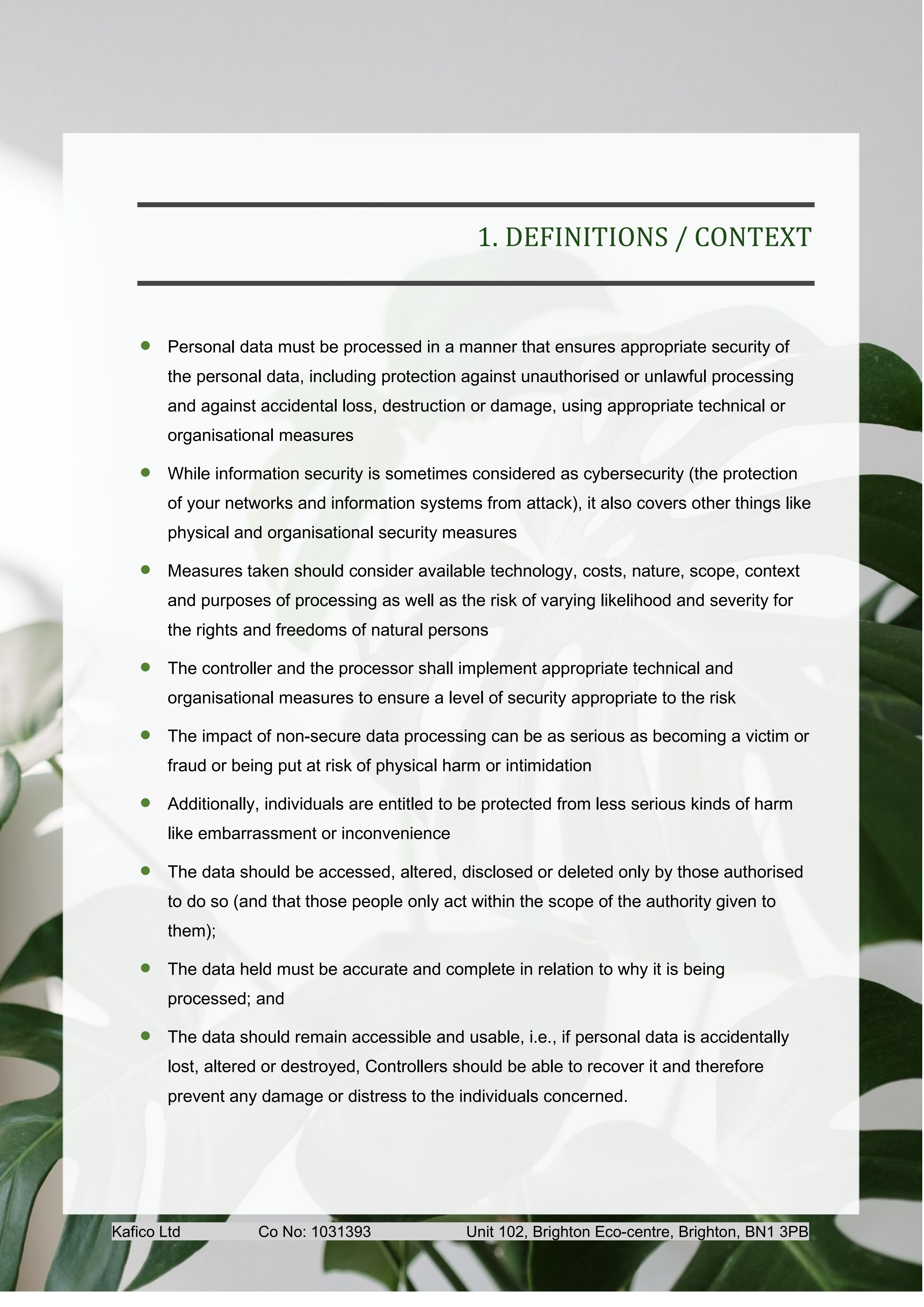
This means that there is low risk of a mismatch between the identifying data (NHS No, Patient Name) and the other extracted items (read codes) when they are pulled back together to facilitate the identification of a particular patient.

There have been no mismatches of this data since the system inception in 2011. The only example where a mismatch between the extracted data and the patient identity would be possible is where the wrong NHS No has been attributed to the patient within the source data and this is outside the scope of control for PSL.

TECHNICAL AND ORGANISATIONAL MEASURES

KAFICO

INFORMATION · GOVERNANCE · CONSULTANCY



1. DEFINITIONS / CONTEXT

- Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures
- While information security is sometimes considered as cybersecurity (the protection of your networks and information systems from attack), it also covers other things like physical and organisational security measures
- Measures taken should consider available technology, costs, nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons
- The controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk
- The impact of non-secure data processing can be as serious as becoming a victim or fraud or being put at risk of physical harm or intimidation
- Additionally, individuals are entitled to be protected from less serious kinds of harm like embarrassment or inconvenience
- The data should be accessed, altered, disclosed or deleted only by those authorised to do so (and that those people only act within the scope of the authority given to them);
- The data held must be accurate and complete in relation to why it is being processed; and
- The data should remain accessible and usable, i.e., if personal data is accidentally lost, altered or destroyed, Controllers should be able to recover it and therefore prevent any damage or distress to the individuals concerned.

2. PROPORTIONALITY

In accordance with the above risk assessment, the project has been defined as having a GOLD degree of risk to the rights and freedoms of data subjects in the event that appropriate technical and organisational measures are not put in place – based on the nature and volume of the data being processed.

This assessment will therefore explore each of the elements drawn out within data protection legislation for mitigation of those risks such that the residual risk is low enough to support implementation.

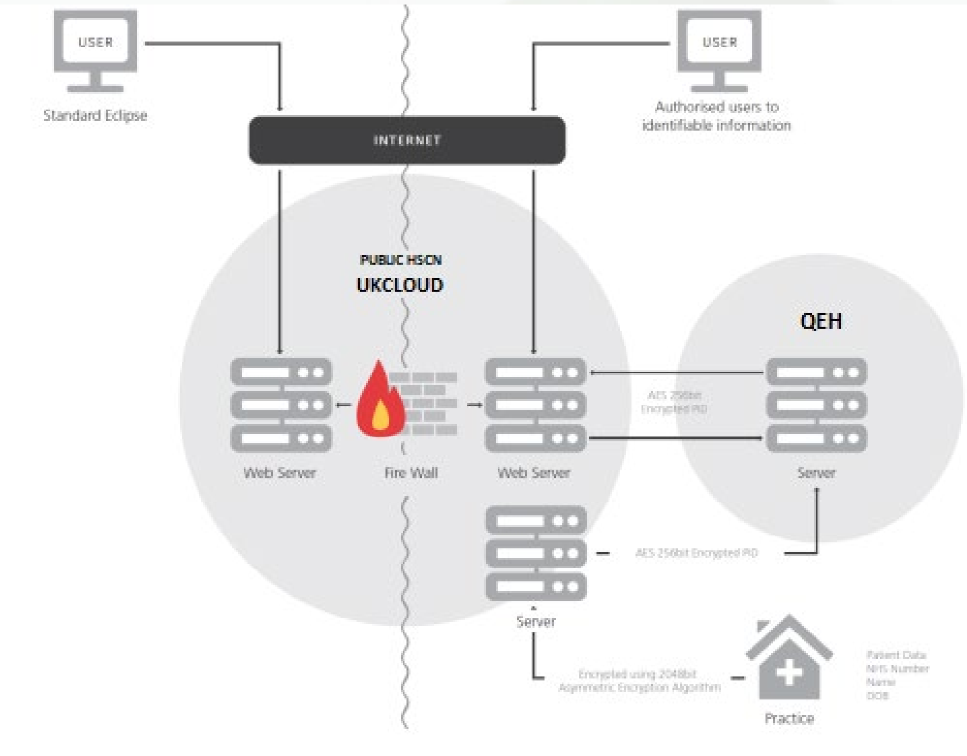
3. SECURITY OF DATA IN TRANSIT AND AT REST

Since the project involves the transfer of data through a network architecture, this assessment has obtained a number of assurances for data in transit in accordance with NHS Digital Cloud Best Practice Guidance.

- Primary care data extracts including some basic demographics (practice code, Patient system reference, gender and age) are fully encrypted to allow secure transmission of data to the PSL high security data centres (UK Cloud) using AES 256bit encryption via TLS V1.2 secure socket connections.
- Identifiable demographic data (patient file, practice code, patient system reference and NHS Number) separately extracted from the practice are also transmitted via TLS V1.2 secure socket connections but these also transferred within the HSCN environment only to the QEHKL Server.
- SUS data transferred from the CSU to secure SFTP site hosted by Prescribing Services Ltd within the HSCN. Secure AES-256bit encryption is utilised for the transmission. Here the data is linked with the Primary Care Data by virtue of the NHS Number which is then replaced with Eclipse no, linked together and saved in QEHKL. The files in the SFTP are then permanently deleted.

- All web access is encrypted using SSL TLS V1.2.

Advice and Guidance (Eclipse Live) employs pseudonymisation and encryption to protect data both in transit and at rest. This is demonstrated below;



Recital 26, the GDPR limits the ability of a data handler to benefit from pseudonymized data if re-identification techniques are "reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly."

To determine how effectively the linked data has been pseudonymised (and therefore further minimised where a large and somewhat speculative data set exists), it is necessary to consider how "reasonably likely" it is that the Controller (or Processor) or another person could directly or indirectly identify a person.

This should consider the time, cost and effort necessary to do so.

The data being held at the QEH Server is;

- Eclipse No (clear)
- Name (encrypted)
- Address (encrypted)

- NHS No (encrypted)
- DOB (encrypted)

All the other data is 256-bit encrypted and they key for which is only available on another server which is hosted at UKCloud

The data held at UKCloud is the linked, pooled data set ***without***;

- Name (encrypted)
- Address (encrypted)
- NHS No (encrypted)
- DOB (encrypted)

And ***with*** the Eclipse Identifier.

This information is also 256-bit encrypted but the decryption key for this information is within the same location and available to a limited number of individuals.

Practice data set extracted manually or by Wellbeing Software (Apollo);

- Demographics
- age (years)
- gender
- clinical system no
- Coded event data
- Clinical sys no
- Read Code (Value 1 value 2)
- Medication data
- medication name
- medication read codes
- Date issued
- status (repeat etc)
- Instructions - free text)

The data is 256-bit encrypted which is regarded as requiring significant cost, time and effort in order to decrypt without the necessary key.

Prescribing Services Ltd services use (where necessary) primary care data extracts imported for the provision of Clinical Decision Support, Risk Stratification and other associated purposes.

This data is imported securely and held in a de-identified form. Safety algorithms are performed on the data and presented to the user. Since the system requires recent primary care data a snapshot of the full primary record set is taken on initiation and frequently updated using delta data uploads prior to risk stratification.

The transfer of data into the into the Prescribing Services architecture uses a defined Data Migration process to safely and efficiently import all primary care data.

It is also worth noting that the data is read coded which provides another layer of protection should the information be inappropriately disclosed.

It is therefore suggested that, due to the de-identification of personal data, creation of a unique integer, encryption and location of the data across multiple locations, the risk of reidentification of the data sets by a motivated intruder is low but a determination and risk assessment will likely be conducted by the Controller(s).

4. PHYSICAL SECURITY

The following security measures have been confirmed as in place for the physical locations of project data;

- Data processed by The Bunker and UKCloud are hosted within industry standard data centres that conform to industry best practices (ISO27001 & G-Cloud IL3) and standards for security as defined in the relevant contract terms and conditions.
- Entry to the PSL premises is via a shared door access through which is controlled by a keypad and code.
- The door is also locked outside of normal working hours and entry to the building is not possible via the keypad alone.

- The company’s office is then accessed by another door which is also controlled by a keypad and code and locked outside of working hours.
- The office servers and communications hardware are located in a server room which is kept locked.
- All visitors are required to sign in and out and be accompanied at all times whilst within the office premises.
- The offices include all fire fighting equipment required under current regulations. These are provided and maintained under the terms of the office occupancy contract.
- Smoke detectors are present throughout the building.
- There is CCTV in place at the PSL premises
- UKCloud has CCTV and Infrared CCTV operating 24 hours a day and covering all operational areas.
- UKCloud has 24/7 security guards on site
- UKCloud has smoke and heat detection and extinguishing systems.
- UK Cloud has backup generators, various uninterrupted power supply feeds and other redundancy such as water and air filtration systems.
- UKCloud has a security card access system
- The Bunker facilities are housed in de-commissioned cold-war era military establishments.
- The Bunker has CCTV and Infrared CCTV operating 24 hours a day and covering all operational areas.
- The Bunker has full EMP shielding to all data floors
- The Bunker has a Borer security card access system
- The Bunker has 24/7 security guards and dogs permanently on site.
- The Bunker has 3m thick walls and 3m high heavy duty security fence topped with barbed wire and is buried 0.5m underground.
- The Bunker has smoke and heat detection and extinguishing systems.
- There are backup generators, various uninterrupted power supply feeds and other redundancy such as water and air filtration systems.

- PSL have confirmed that the QEH Server is within the QEH Hospital and is protected by the hospital’s physical and procedural security controls.
- PSL have confirmed that the QEH server’s access is protected by locked doors and in a server room
- PSL have confirmed that the QEH server is covered by 24/7 CCTV
- PSL have confirmed that the QEH server access is controlled by ID badges and key cards
- PSL have confirmed that the QEH hospital has security guard presence and is protected by fire and smoke detection systems.

5. CLOUD HOSTING – UKCloud

These assurance items are based on the NHS Digital Health and Social Care Cloud Security – Good Practice Guide.

- PSL confirms that they use the VMWare product supplied by UKCloud
- PSL has confirmed that they have taken the steps necessary to ensure that the cryptography offered by UKCloud (VPN AES256 and HTTPS TLS Version 1.2) is in place and active for this project - such that communications between cloud components are encrypted to recognised best practice standards.
- PSL has taken steps to ensure that the max encryption levels offered by UKCloud are active for this project. Such that communications between cloud data centres are encrypted to TLS Version 1.2 or above OR IPsec or TLS VPN gateway as defined by NIST SP800-57.
- PSL has taken steps to ensure that the max encryption levels offered by UKCloud are active for this project. Such that communications between cloud admin portal and the cloud are encrypted to TLS Version 1.2 or above OR IPsec or TLS VPN gateway as defined by NIST SP800-57.
- UKCloud undertakes annual assessments against recognised standards such as ISO to test the security of the cloud communications.
- UKCloud architecture utilises strong cryptography as defined by NIST SP800-57 to encrypt communications between the Cloud and the End-user (TLS Version 1.2)
- PSL undertakes regular (minimum yearly) penetration testing of the communication between the Cloud and the End-user, ensuring that the Penetration test is well scoped such that ‘Data in transit protection’ is fully tested.
- The UKCloud Region is set to Farnborough, with backups being stored in the AWS London EU-WEST-2 data centre.

- UKCloud provides the ability to apply encryption facilities to ensure that no data is written to storage in an unencrypted form. The provider has ensured that this facility is active for this project.
- The provider confirms that the project utilises strong cryptography for data at rest as defined by the current version of NIST SP800-57
- PSL confirms that the data at rest encryption is tested annually against a recognised standard such as ISO or FIPS 140-2 to test the encryption strength.
- PSL has its servers on “warm standby” which are servers which could be initiated within 2 hours for any server failure. This configuration is set up in the same data centre. Should the data centre location suffer a total outage, PSL have the resources in place to set up the servers in another zone, and expect it would take about 4 hours.
- UKCloud has firewall protection which has been configured and enabled.
- UKCloud has given assertions regarding their data sanitisation approach for cloud storage. If the customer needs a specific standard/method of sanitisation such as DoD 5220.22-M (“National Industrial Security Program Operating Manual “) or NIST 800-88 (“Guidelines for Media Sanitization”) the PSL will use a secure delete tool which behaves on the UKCloud storage in the same way it would on a local physical disk.. PSL has confirmed they will delete data on request of the controller and that the appropriate deletion tool will be used in accordance with the risk posed by the data therein. PSL has a destruction policy as part of their ISO27001 certification.
- Regarding equipment disposal, UKCloud is certified with ISO/IEC 27001:2013, and CSA STAR Level 1
- UKCloud security protections and control processes (including sanitisation) are independently validated by multiple third-party independent assessments: https://ukcloud.com/governance/
- UKCloud operates data centers in alignment with the Tier III+ guidelines, and guarantee an up time of 99.9999%> (excluding planned maintenance).

6. CLOUD HOSTING – The Bunker

These assurance items are based on the NHS Digital Health and Social Care Cloud Security – Good Practice Guide.

This assurance relates to the following PSL services;

- ✓ Eclipse Development Analytics

- PSL confirms that they use the VMWare product supplied by UKCloud
- PSL has confirmed that they have taken the steps necessary to ensure that the cryptography offered by The Bunker (VPN AES256 and HTTPS TLS Version 1.2) is in place and active for this project - such that communications between cloud components are encrypted to recognised best practice standards.
- PSL has taken steps to ensure that the max encryption levels offered by The Bunker are active for this project. Such that communications between cloud data centres are encrypted to TLS Version 1.2 or above OR IPsec or TLS VPN gateway as defined by NIST SP800-57.
- PSL has taken steps to ensure that the max encryption levels offered by The Bunker are active for this project. Such that communications between cloud admin portal and the cloud are encrypted to TLS Version 1.2 or above OR IPsec or TLS VPN gateway as defined by NIST SP800-57.
- The Bunker undertakes annual assessments against recognised standards such as ISO to test the security of the cloud communications.
- The Bunker architecture utilises strong cryptography as defined by NIST SP800-57 to encrypt communications between the Cloud and the End-user (TLS Version 1.2)
- PSL undertakes regular (minimum yearly) penetration testing of the communication between the Cloud and the End-user, ensuring that the Penetration test is well scoped such that ‘Data in transit protection’ is fully tested.
- The Bunker Region is set to Berkshire with backups being stored in the AWS London EU-WEST-2 data centre.

- The Bunker provides the ability to apply encryption facilities to ensure that no data is written to storage in an unencrypted form. The provider has ensured that this facility is active for this project.
- PSL confirms that the project utilises The Bunker utilises strong cryptography for data at rest as defined by the current version of NIST SP800-57
- PSL confirms that the data at rest encryption is tested annually against a recognised standard such as ISO or FIPS 140-2 to test the encryption strength.
- PSL has servers on “warm standby” which are servers which could be initiated within 2 hours for any server failure. This configuration is set up in the same data centre. Should the data centre location suffer a total outage, PSL have the resources in place to set up the servers in another zone, and expect it would take about 4 hours.
- The Bunker has firewall protection which has been configured and enabled.
- The Bunker has given assertions regarding their data sanitisation approach for cloud storage. If the customer needs a specific standard/method of sanitisation such as DoD 5220.22-M (“National Industrial Security Program Operating Manual “) or NIST 800-88 (“Guidelines for Media Sanitization”) the PSL will use a secure delete tool which behaves on the UKCloud storage in the same way it would on a local physical disk.. PSL has confirmed they will delete data on request of the controller and that the appropriate deletion tool will be used in accordance with the risk posed by the data therein. PSL has a destruction policy as part of their ISO27001 certification.
- Regarding equipment disposal, The Bunker is certified with ISO/IEC 27001:2013, and CSA STAR Level 1
- The Bunker security protections and control processes (including sanitisation) are independently validated by multiple third-party independent assessments: https://www.thebunker.net/compliance/
- The Bunker operates data centers in alignment with the Tier III+ guidelines, and guarantee an up time of 99.9999%> (excluding planned maintenance).

7. DATA SUBJECT USER AUTHENTICATION

There is no data subject access to systems or data.

8. PROFESSIONAL USERS - AUTHENTICATION

To ensure that the authentication of professional users of the system is in line with Gov.UK and NIST standards, the following assurances have been sought and confirmed;

- Most users use NHS Pathways credentials logging into the system.
- Professional user log in is multi-factor. The user logs in using a username and password and then uses a code received from an SMS/Email.
- For professional users, the password at least 8 characters long but does NOT set a maximum length.
- For professional users, when password is changed, the user receives an alert making them aware that their password has recently been changed?
- For professional users, the system explains the password constraints to professional users
- For professional users, the system gives professional users 5 attempts to enter their password correctly before locking their account or do any further security checks.
- For professional users, the system hides professional user passwords by default
- For professional users, the system allows the professional user to paste their password
- For professional users the Passwords of professional users stored salted and hashed, using algorithms and strengths recommended in NIST Cryptography Standards

- For professional users, when a professional user enters their account details incorrectly, the system conceals whether they got the username or password wrong.
- For professional users, when locked out or changing password, the professional user is sent a time-limited password-reset code to the phone number or email that they registered with that does not use password reset questions and does not use password reminders.
- For professional users, when a password is changed, the professional user receives an alert making them aware that their password has recently been changed.
- The software allows different privileges for different job roles
- For professional users, when a professional user is logged in, the organisation that they are logged in under presents itself on screen throughout their use of the system.
- For professional users, professional users have cannot have more than one role per login.

It has been confirmed that Prescribing Services would only ever access personal data in the following scenarios;

When a clinical customer requires technical support, or if they have put the format of a date of birth in incorrectly for example. The users will call the CCG and then the CCG will come to PSL. PSL does not deal with patients/customers direct under normal protocol.

9. SYSTEM AUDIT

The project introduces a system or software that professional users directly access and so there is a need to ensure that the audit functionality for the asset is appropriate such that transparency is supported and Administrators have the necessary oversight.

The following assurances have been sought and obtained;

- All systems / software enables and supports investigations for any reason (e.g. inappropriate access or cyber security incident)

- The system / software allows identification of any changes which have been made to clinical or administrative data, Patient/Service User data. This includes identifying what changes were made, by what user and at what time.
- The systems provide completed auditing:
  - Username (Where logged in)
  - Time of event
  - Activity undertaken
  - IP address of action
  - Duration of activity
- The systems allow monitoring of whether access controls are working as intended. Administrators may audit the movements of all staff, so it is possible to check that they are not accessing areas which they shouldn't be or seeing things or doing things they shouldn't be.
- System audit trail includes updates, backups, any maintenance activities or reference data changes.
- For successful login audit data includes User ID, date and time (hh:mm:ss)
- For unsuccessful login audit data includes number of attempts, Date and time, Access point (if available), User ID (if available)
- The Password Change audit data includes User ID, User whose password was changed, Date and time, end-user device (or Solution) identification information

10. INTERNATIONAL TRANSFERS

All data sets have UK regions selected.

Customer / patient data does not leave the UK.

11. DUE DILIGENCE

The stakeholders have achieved the following accreditations that assist to reduce the risk to the rights and freedoms of data subjects;

- PSL has completed a compliant NHS Data Protection and Security Toolkit for the current year available at PSL Toolkit
- PSL has achieved ISO27001 accreditation – certificate number 1412892
- Wellbeing Software has completed a compliant NHS Data Protection and Security Toolkit for the current year available at Wellbeing Toolkit
- Wellbeing Software has achieved ISO27001 accreditation as confirmed via Wellbeing ISO27001
- The Bunker has submitted a compliant NHS Data Protection and Security Toolkit for the current year available at The Bunker Toolkit
- The Bunker has achieved ISO27001 accreditation as confirmed via The Bunker ISO27001
- UK Cloud has submitted a compliant NHS Data Protection and Security Toolkit for the current year available at UKCloud Toolkit
- UKCloud has achieved ISO27001 accreditation as confirmed via UKCloud Governance

As part of the impact assessment, a review of media coverage was undertaken to determine whether there have been reports of breaches or complaints relating to suppliers or partners involve in the service delivery.

At the time of writing no stakeholders had no media presence with regards to data breaches.

Checks have been undertaken with regards to the UK Information Commissioner and all parties, where relevant, are registered and their registrations are below

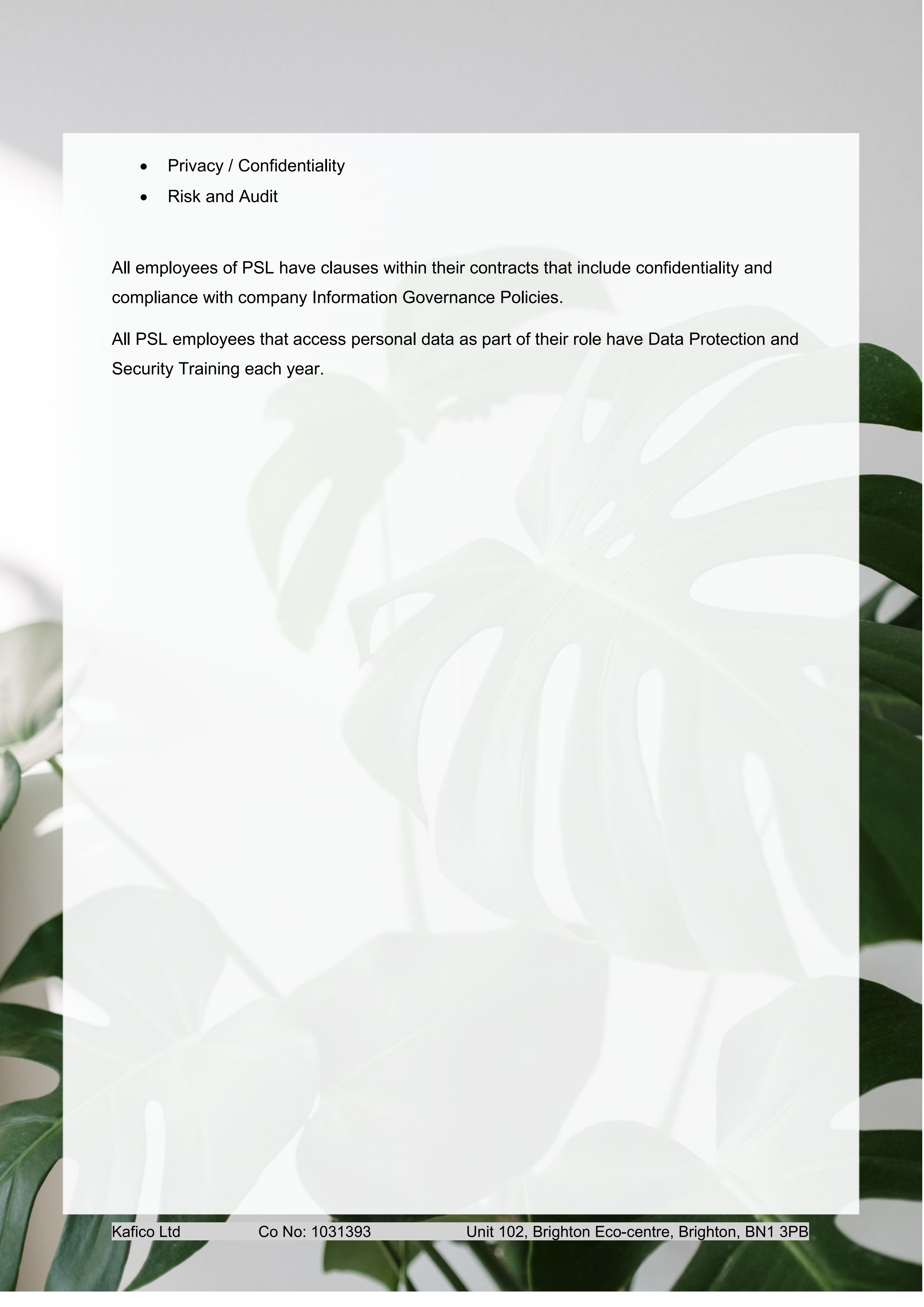
- PSL are registered with the ICO under the registration number Z2536678
- Wellbeing Software are registered with the ICO under the registration number ZA640896
- The Bunker are registered with the ICO under the registration number Z8856975
- UKCloud are registered with the ICO under the registration number Z2926991

The stakeholders have identified the following leads for data protection matters;

- Prescribing Services Ltd - Emma Cooper - emma.cooper@kafico.co.uk
- Wellbeing Software - wellbeingservice@wellbeingsoftware.com
- The Bunker - Christopher.scott@thebunker.net
- UKCloud - dpo@ukcloud.com

PSL have policies that cover the following subjects;

- Information Governance
- Data Protection Impact Assessments
- Data Subject Rights
- Information Incidents
- Information Security



- Privacy / Confidentiality
- Risk and Audit

All employees of PSL have clauses within their contracts that include confidentiality and compliance with company Information Governance Policies.

All PSL employees that access personal data as part of their role have Data Protection and Security Training each year.