Cookbook for Regional Interoperability Detailed Design Paper #015

Governance for Data Consumers

Version 1.1 – 28th September 2021

Abstract Interoperability Cookbook Anchor Points

Section	Title
5	Requirements for Data Consumers

Table of Contents

Version Control

Version	Release Date	Released By	Reason for Release
1.0	03/05/2020	R Hickingbotham	Preliminary draft
1.1	28/09/2021	T Davey	Add further details of cyber assurance

Reviewers

Initials	Name	Role	Organisation

1 Introduction

1.1 Purpose of this Document

This document is one of a series of design papers which underpin the Abstract of a Cookbook for Regional Interoperability (the Abstract Cookbook). These papers, in their totality, describe the technical components and the standards which form the YHCR System of Systems (SoS). They are intended as a basis for developing or procuring software and so are expressed at a level of precision which aims to avoid ambiguity but consequentially, they are focussed to technical readers.

Design papers are anchored to topics which are discussed in the Abstract Cookbook. They are elaborations of the concepts which were first introduced by the abstract and new content is further detail rather than variations of previously established core principles.

This document (design paper 015 - “Governance for Data Consumers”) draws together governance requirements that are discussed in other design papers and presents them in a single source. It is a companion paper to design paper 014 – "Governance for Data Providers".

The paper only addresses governance from the perspective of being a member of the YHCR. It does not attempt to fully define IT governance and it assumes that the requirements presented here are underpinned by established governance processes that allow the data consumer to contribute as an effective and legislatively compliant member of the NHS or supplier to it.

1.2 Relationship of this Document with Other Standards

This paper does not require knowledge of any particular standard.

1.3 Intended Users of the This Document

Organisations operating as data consumers.

2 Governance Checklist

References in the following requirements are to the design paper which provides further detail. Relevant design papers are listed at the end of the section

Information Governance

i. Authenticate users in compliance with an identity management policy which provides a high degree of confidence that a person accessing the YHCR can be identified and is authorised to do so. (016)
ii. Assign users a role which is appropriate for their job function and restrict access to the YHCR to roles which have an appropriate reason for access. (005)
iii. Implement measures to ensure that users accessing the YHCR have a legitimate relationship with the patient whose data is being accessed. These may include self-regulation backed up by appropriate training and capturing statements from users, or systematically enforced controls. (016)
iv. Ensure that users who make subscriptions to patient cohorts for the purpose of direct care either have a legitimate relationship with all members of the cohorts or notifications must be discarded for patients where the subscriber does not have a legitimate relationship. (007)
v. Discard transactional messages which are incorrectly received for patients for the which the organisation does not have a current legitimate relationship. (006)
vi. Log as audit data all access requests made to the YHCR (including synchronous queries, asynchronous queries, subscriptions registered, subscription notifications received, and transactional messages received). Include the YHCR supplied bearer-token (JWT) as a searchable key to audit data. (009)
vii. Store audit data as either FHIR Audit resources persisted in a FHIR repository connected as a data provider to the YHCR or implement a service for responding to data access requests. (009)
viii. Backup audit data. (028)
ix. Periodically (at least weekly) review logs of usage of the YHCR and investigate unusual patterns of behaviour. (016)
x. Implement a data retention policy for audit data which is aligned to the YHCR's requirement and delete data in accordance with the policy. (016)

Security

xi. Use the YHCR IAM service to obtain separate bearer tokens for each user requiring access to the YHCR. (005)
xii. Set expiry times for assertions to IAM in accordance with YHCR policy. (005)
xiii. Declare a reason for access and user role in assertions that reflect users' utilization of YHCR data. (005)
xiv. Refresh bearer tokens before their expiry date. (005)
xv. Restrict trusted certificating authorities on endpoints accessible by the SoS to the YHCR CA. (016)
xvi. Authenticate certificates served from all YHCR endpoints. (016)
xvii. Use certificates signed by the YHCR and rotate certificates in accordance with YHCR policy. (016)
vii. Maintain a recognised accreditation of cyber security good-practice, consisting of at least ONE of:
    - Cyber Essentials or Cyber Essentials Plus
    - ISO 27001
    - IASME

For partner organisations using ONLY the Portal then in addition acceptable options include at least ONE OF:

- DSP Toolkit
- PSN Code of Connection

(Note: In the exceptional event that no appropriate certifications are held then an alternative is offered – based on a checklist of questions covering similar ground and targeting: networks, firewalls, security, and patching. Evidence is captured as part of the Onboarding Process and would need to be reviewed and specifically approved as an exception at Shared Care Record Board level prior to go live).

viii. Provide additional evidence of Device Management good-practice. Evidence is gathered via a checklist as part of the Onboarding process, with a positive response required on each point and any exceptions requiring signoff at Shared Care Record Board level.

<u>For subscription notification and reliable messaging endpoints</u>

xviii. Check access tokens included in all data requests from the YHCR. Validate that tokens are signed by the YHCR and are active. (005)

xix. Restrict trusted certificating authorities on endpoints accessible by the SoS to the YHCR CA. (016)

xx. Whitelist only IP addresses permitted to access YHCR services. (016)

Performance and Availability

xxi. Implement services which are designed with recognition of the performance objectives for the YHCR. (028)

xxii. Implement services which are tolerant of performance constraints at data providers and respond appropriately to an *OperationOutcome* notifying the consumer of temporary unavailability of a data provider. (028)

xxiii. Use the asynchronous query interaction type for bulk data requests. (010)

xxiv. Use the data availability service to determine whether the YHCR has data for a patient. (002)

xxv. Design data consumers to interact efficiently with the YHCR and optimise use of query directives to reduce the number of interactions required to obtain data. (003)

xxvi. Use result pagination to control the number of items requested from the YHCR. (003)

Governance Structures

xxvii. Operate a 2nd line support operation for resolving issues with local data consumption.

xxviii. Supply a representative to the YHCR Management Board.

Compliance

xxix. Interpret data in a manner that is cognisant of the maturity level of each data provider. (023)

xxx. Use data impairments reported in query results to inform users appropriately of possible data incompleteness or other deficiencies in data. (017)

xxxi. Aggregate or de-duplicate data in a manner which is appropriate for usage of the data consumer. (026)

xxxii. Inform users of data provides by the YHCR which has restricted status. (008)

Change Management

xxxiii. Operate a change assurance board.

xxxiv. Inform the YHCR of planned changes to services or systems and infrastructure on which they depend at least 7 days before the change is to be applied.

xxxv. Implement a process for receiving change notices from the YHCR change assurance board and evaluating impact on local services.

xxxvi. Maintain a functionally stable service and implement enhancements through the onboarding of new product versions. (021)

Design Papers

002 Data Availability Service
003 Conceptual Design for a FHIR Proxy Server
005 Identity and Access Management (IAM) Service
006 Reliable Messaging Infrastructure
007 Subscriptions Infrastructure
008 Data Access and Consent Management
009 Auditing
010 FHIR Aggregator Service
016 Securing the YHCR
017 Data Quality Reporting
021 Onboarding Data Consumers
023 The YHCR Maturity Model
026 Data Normalisation
028 Non-Functional Requirements for Regional Infrastructure

Appendix 1 – Maturity Matrix

Section	Narrative	Consultative	Draft	Normative
1 Introduction 1.1 Purpose of this Document	X			
1.2 Relationship of this Document with Other Standards	X			
1.3 Intended Users of this Document	X			
2 Governance Checklist			X	