
# Cookbook for Regional Interoperability Detailed Design Paper #014

# Governance for Data Providers

Version 1.1 – 28th September 2021

**Abstract Interoperability Cookbook Anchor Points**

| Section | Title |
|---|---|
| 4 | Requirements for Data Providers |
| | |

# Table of Contents

## Version Control

| Version | Release Date | Released By | Reason for Release |
|---|---|---|---|
| 1.0 | 26/04/2020 | 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 014 - “Governance for Data Providers”) 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 015 – "Governance for Data Consumers".

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 provider 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 providers.

# 2 Governance Checklist

**Information Governance**

i. Log as audit data all requests for data from the YHCR and data items released to the YHCR. (009)
ii. Implement a retention policy for audit data that complies with the retention requirements specified in the YHCR Operations Guide. (016)
iii. Restrict access to FHIR Audit resources data to requestors with a role of "Auditor". (005)
iv. Implement either searchable FHIR Audit resources or a service for responding to data access requests. (009)
v. Formulate and enforce data access policies which govern the scope of data available over the YHCR. (008)
vi. Enforce local consent policies or register local consent policies with the YHCR for regional enforcement. (008)
vii. Ensure that data distributed using the YHCR reliable messaging channel is directed at an organisation with a legitimate relationship with the subject. (006)

**Security**

vii. Check access tokens included in all data requests from the YHCR. Validate that tokens are signed by the YHCR and are active. (005)
viii. Restrict trusted certificating authorities on endpoints accessible by the SoS to the YHCR CA. (016)
ix. Whitelist only IP addresses permitted to access YHCR services. (016)
x. Rotate certificates in accordance with YHCR policy. (016)
xi. Maintain a recognised accreditation of cyber security good-practice, consisting of at least ONE of:
    - Cyber Essentials or Cyber Essentials Plus
    - ISO 27001
    - IASME

    (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).
xii. 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.

**Performance and Availability**

xi. Implement services which operate within the performance objectives for the YHCR. (028)
xii. Backup data and implement a disaster recovery procedure that is designed to recover a service within 4 hours. (028)
xiii. Implement a high availability architecture for live services. (028)

**Governance Structures**

xiv. Operate a 2nd line support operation for resolving issues with local data provision.

xv. Supply a representative to the YHCR Management Board.

**Compliance**

xvi. Adhere to a published maturity level for technical capability and data content. (023)
xvii. Maintain connectivity from the YHCR system test environment to test services which, whilst not necessarily highly available, are operated to production standards. (020)
xviii. Populate test services with a YHCR defined bank of test patients and representative data aligned with the data content definitions of the declared maturity level. (020)
xix. Only register patient/client contact with the YHCR where the NHS number which has been traced against the Patient Demographic Service. (004)
xx. Report data impairments as measured against the declared maturity level in search requests. (017)
xxi. Only provide data to the YHCR where the provenance is uniquely that of the data providing organisation. (026)

**Change Management**

xxii. Operate a change assurance board.
xxiii. 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.
xxiv. Implement a process for receiving change notices from the YHCR change assurance board and evaluating impact on local services.
xxv. Maintain a functionally stable service and implement enhancements through the onboarding of new product versions.

**Design Papers**

002 Data Availability Service
003 Conceptual Design for a FHIR Proxy Server
004 Patient Identity Exchange (PIX)
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
020 Onboarding Data Providers
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**<br>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 | |