Digital Child Health Architecture

Mike Kelly

Draft - Published 10 November 2016

**Contents**

[1 Introduction 3](#_Toc475001914)

[1.1 Background 3](#_Toc475001915)

[1.2 Key Drivers 5](#_Toc475001916)

[1.3 Architecture Scope 6](#_Toc475001917)

[2 Events 8](#_Toc475001918)

[3 Events Catalogue 9](#_Toc475001919)

[4 Events Test Service 10](#_Toc475001920)

[5 Registration Service 11](#_Toc475001921)

[6 Events Management Service 12](#_Toc475001922)

[7 Failsafe Management Service 16](#_Toc475001923)

[8 Professional Identity Services 20](#_Toc475001924)

[9 Citizen Identity Services 21](#_Toc475001925)

[10 Citizen 2 Citizen Relationship Services 22](#_Toc475001926)

[11 Citizen 2 Professional Relationship Service 23](#_Toc475001927)

[12 Electronic Personal Child Health Record 24](#_Toc475001928)

# 1 Introduction

This document provides an overview of the architecture of the services to support the Digital Child Health (DCH) Programme. The architecture is based on the vision statement expressed in the Children’s Health Strategy. As part of the discovery phase of DCH the assumptions of the vision are being tested and elaborated. Therefore the architecture expressed in this document should be treated as a candidate architecture only, and dependant on the outputs of the discovery phase may change.

The architecture should be treated as a conceptual architecture. An actual logical and physical architecture will be based on existing and planned national capabilities.

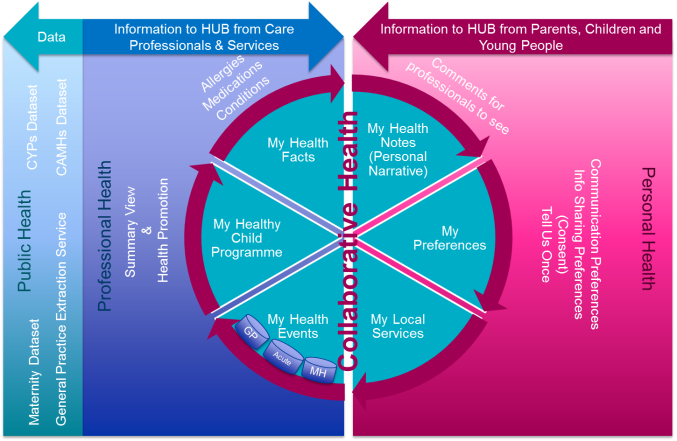
## 1.1 Background

The Children’s Health Digital Strategy is commissioned by NHS England and was published Q4 2016.

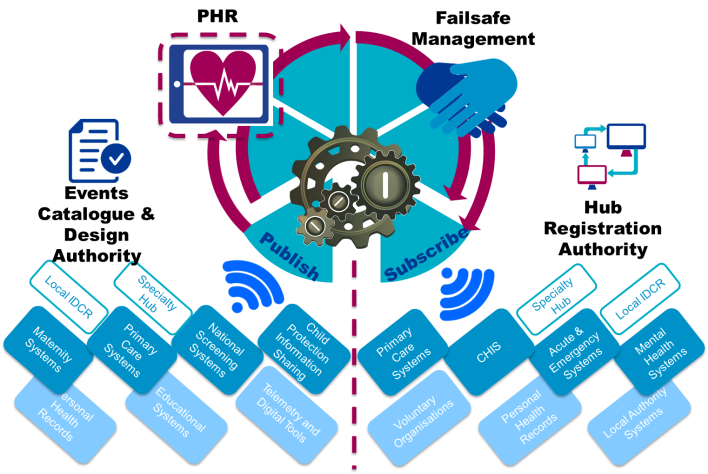
It sets out the case for transforming the way information is handled in children’s health services. It suggests that making health information interoperable – translating it into messages which can be exchanged – and ensuring that we effectively manage the offer and uptake of preventative programmes of care is the best way of achieving the key objectives of:

* Knowing where every child is and how healthy they are
* Giving appropriate access to information for all involved in the care of children

The strategy contains a vision for a Digital Child Health Hub:



The strategy also defines a set of Digital Services that are intended to be delivered, which are based on an Events Hub model:



The Digital Services are:

1. **Child Health Events Catalogue** - Child Health do not need to exchange whole care records only small event messages so the information can flow to whoever needs it in the eco system in real time. There will be multiple event types; transactional events, clinical events, consent events.
2. **Events Management Service** - A service that facilitates the exchange of messages between publishers of event information and subscribers to that information in real time.
3. **Failsafe management of the child population** - Event information and rules service, will manage both population tracking and population screening. Will tell systems location and which professionals/agencies a child is under the care of. Will prompt parents and professionals to attend for/deliver the standard programme of care and will alert if not delivered/undertaken. Needed to prevent children missing care.
4. **Digital Personal Child Health Record (ePCHR)** - Child-centric untethered PHR, needs to meet the current standards laid down by the Royal College of Paediatrics and Child Health for what constitutes an ePCHR. Significant strategic opportunity to advance self-care agenda and to join up maternity and new-born healthcare as per Maternity review by extending timeline for PHR backwards to include mother’s health.

The responsibility to deliver these Digital Services has been given to NHS Digital via the Digital Child Health Programme, which is a NIB Domain G (Paper Free at Point of Care) programme.

## 1.2 Key Drivers

The following are the key drivers from the strategy that identify the investment objectives and inform the architecture.

New information services for parents, families, carers, children and young people:

1. Parents, families and carers will have an online record of their child’s health and development.
2. Young people will have an online record of their own health and care issues.
3. There is a common (core) view of the health information recorded about children and young people in different health and care organisations that is shared by parents, families, carers, children, young people and professionals.
4. Parents, families, carers, children and young people can set their own preferences for information sharing and can see who subscribes to their information.
5. Parents, families, carers, children and young people can publish their own goals for health and wellbeing and share these with professionals.

New information services for professionals:

1. Professionals will have access to a core view of child health information at the point of care.
2. Up to date health events will be available in their own health record systems, they will not need to access other systems.
3. Professionals with a responsibility for a child will have real time access to events occurring for that child in other organisations, where it is appropriate to do so.
4. Professionals will only have to record information about a child/young person once as that information can then be published automatically to those in the extended network of care.
5. A failsafe management service will make it easier to identify when a child has fallen outside of the care of the usual responsible agencies, such as a GP or Health Visitor.
6. A failsafe management service will alert those delivering preventative programmes of care when an intervention is due or has been missed.

New information services for public health:

1. Public health professionals will have access to more comprehensive, more up to date datasets as interoperability of events gradually replaces the re-keying of information from paper notifications.
2. Administration of public health programmes and call and recall can be standardized to a high degree through applying immunisation rules and schedules nationally as a series of events rather than locally.
3. As interoperability of events becomes routine, public health professionals will have access to real time population data for analysis.
4. As parents, families, carers and young people begin to use personal health records routinely, it becomes possible to deliver personalized health promotion materials to people and enter into dialogue with them.

## 1.3 Architecture Scope

The architecture scope is:



The key actors using this architecture are:

* System Suppliers – suppliers of IT systems used by health and care providers.
* Health and Care Service Providers – organisations that deliver health services and social care services. They will be using systems from System Suppliers.
* Child Health Record Departments – organisations that are commissioned to manage the health of children in their region. They will be using systems from System Suppliers.
* Electronic Personal Child Health Record Providers – organisations that offer an ePCHR for use by citizens. They will be using systems from System Suppliers.

# 2 Events

In the proposed Events Hub model, information that needs to be exchanged is broken down into small parcels of information that are termed ***Events***. These will be modelled as FHIR resources.

Events are sent (published) by the IT systems used by service providers in real time to a national hub run by the NHS (Events Management Service).

Other IT systems that have a need for these events create subscriptions on the hub defining what types of event they want.

When the hub receives an event from a publisher it matches it to subscribers and sends it to them in real time.

An ***Event Type*** will be a formal specification for a type of event (a FHIR resource profile). The ***Events Catalogue*** is the collection of all these specifications.

# 3 Events Catalogue

The ***Events Design Authority*** (***EDA***) will be part of NHS Digital. Its role is to govern and maintain the Child Health Events Catalogue. To do this it will have five key functions:

1. Governance - select and prioritise development of new event types
2. Requirements - develop event type requirements
3. Specifications - develop event type specifications
4. Publication - provide a public website on which the events catalogue is published
5. Testing - provide a public test service which can be used by system developers

The EDA will maintain a public (Internet facing) website on which all assets are published. This will include:

* Basic information about the EDA
* Pipeline of new Event Type developments
* Events Catalogue containing:
  + Event Type Requirements
  + Event Type Specifications
* Event Test service information
* How to propose a New Event Type information

# 4 Events Test Service

The EDA will maintain a public (Internet facing) test service. This will provide a RESTful API that allows system suppliers to:

* Send a request for a test event message for a specific Event Type. The response will be a test event message.
* Send a test event message for a specific Event Type. It will be validated, checked that it conforms to the ETS. The response will contain the validation result.

This may be a totally open access service or may require a system supplier to register to obtain an access key to use.

This will be a free service.

There will be no associated service level agreements, it is provided on a best endeavours basis, and there are no guarantees on availability or performance of the service. It is intended to provide a simple test service for initial functional testing. It is not intended for non-functional testing.

# 5 Registration Service

A registration service run by NHS Digital will provide the following key functions:

1. Accreditation/Assurance of suppliers IT systems to connect to and use DCH services
2. Approval of organisations (Health and Care Service Providers, Child Health Record Departments, and Electronic Personal Child Health Record Providers) to connect to and use DCH services
3. Monitoring of use of DCH services by organisations

# 6 Events Management Service

The Events Management Service facilitates the exchange of messages between publishers of event information and subscribers to that information in real time.

It is broken down into the key capabilities shown below:



#### Receive Event Management

Receive an event from a channel, validate it is correct and check the policy for the producer (managed by the service) that they are allowed to send this event type. Send an appropriate response back through appropriate channel as configured for the producer (managed by the service). Audit everything in the Log.

Receive a request to query what events a producer has published to the service, validate it is correct and check the policy for the producer (managed by the service) that they are allowed to query. Send the query results back through appropriate channel as configured for the producer (managed by the service). Audit everything in the Log.

#### Event Producer I/O

Provide multiple I/O channels that allow an external producer system to interact with Receive Event Management. This should include Restful, SOAP, email and file transfer. The interactions can include individual or batched events.

Network accessible from public sector networks and the Internet.

End point authentication from public sector networks and the Internet.

Authenticate all interactions and protect all I/O channels from attack vectors. Based on the identity of the external producer system check policy/configuration (managed by the service) that producer can use the channel. Audit everything in the Log.

For batched events, split them into individual events before passing to Receive Event Management. Audit everything in the Log.

For responses that are configured to be batched, aggregate individual responses from Receive Event Management into a batched response. Audit everything in the Log.

#### Event Subscription Management

Receive a create subscription from a channel, validate it is correct and check the policy for the subscriber (managed by the service) that they are allowed to create this subscription template. Send an appropriate response back through appropriate channel as configured for the subscriber (managed by the service). Audit everything in the Log.

Where a subscription is retrospective, tell the Publication and Subscription Engine. Audit everything in the Log.

Receive a request to query what subscriptions subscriber has created on the service, validate it is correct and check the policy for the subscriber (managed by the service) that they are allowed to query. Send the query results back through appropriate channel as configured for the subscriber (managed by the service). Audit everything in the Log.

Receive a delete subscription from a channel, validate it is correct and check the policy for the subscriber (managed by the service) that they are allowed to delete a subscription. Send an appropriate response back through appropriate channel as configured for the subscriber (managed by the service). Audit everything in the Log.

#### Event Subscriber I/O

Provide multiple I/O channels that allow an external subscriber system to interact with Event Subscription Management. This should include Restful, SOAP, email and file transfer. The interactions can include individual or batched subscriptions.

Network accessible from public sector networks and the Internet.

End point authentication from public sector networks and the Internet.

Authenticate all interactions and protect all I/O channels from attack vectors. Based on the identity of the external subscriber system check policy/configuration (managed by the service) that subscriber can use the channel. Audit everything in the Log.

For batched subscriptions, split them into individual subscriptions before passing to Event Subscription Management. Audit everything in the Log.

For responses that are configured to be batched, aggregate individual responses from Event Subscription Management into a batched response. Audit everything in the Log.

#### Send Event Management

Support both a push model to send events to consumers and a pull model to allow consumers to retrieve send events that are waiting for them.

Send an event through appropriate channel as configured for the consumer (managed by the service). Audit everything in the Log.

Receive a retrieve request, validate it is correct and check the policy for the consumer (managed by the service) that they are allowed to retrieve. Send the events back through appropriate channel as configured for the consumer (managed by the service). Audit everything in the Log.

#### Event Consumer I/O

Provide multiple I/O channels that allow an external consumer system to interact with Send Event Management. This should include Restful, SOAP, email and file transfer. The interactions can include individual or batched events.

Network accessible from public sector networks and the Internet.

End point authentication from public sector networks and the Internet.

Authenticate all interactions and protect all I/O channels from attack vectors. Based on the identity of the external consumer system check policy/configuration (managed by the service) that consumer can use the channel. Audit everything in the Log.

For responses that are configured to be batched, aggregate individual responses from Send Event Management into a batched response. Audit everything in the Log.

#### Channel Management

Some external end points may have constraints on availability and capacity that the service needs to be aware of when for example sending events to consumer systems. Provide an end point directory with configurable availability / throughput throttle / quota for each end point that is used by all the Event I/O channels where appropriate. Audit everything in the Log.

Some external end points may have a charging mechanism based on each transaction / interaction. Provide an end point directory with configurable interaction cost (end point system charge and service charge) for each end point. As part of configuration for producers, subscribers and consumers allow setting of spend limits. Meter channel usage and disable end point use for producer, subscriber or consumer if spend limit exceeded, as well as notifying them. Audit everything in the Log.

Provide billing to charge producers, subscribers and consumers for usage. Audit everything in the Log.

Provide payment engine to receive payments from producers, subscribers and consumers for usage. Audit everything in the Log.

#### Publication and Subscription Engine

Receive event from Receive Event Management. Send to Event Archive. Find all the subscriptions that match the event from Event Subscription Management. For each consumer with a subscription, replicate event and address to consumer. Check there are permissions (managed by the service) – both data sharing and consent – to allow sending to consumer. Where the subscription template defines anonymisation or pseudo anonymisation, this is applied. Pass events to Send Event Management. Audit everything in the Log.

Receive notification of retrospective subscription from Event Subscription Management. Get subscription from Event Subscription Management and pass to Event Catch-up. For each event returned address to consumer. Check there are permissions (managed by the service) – both data sharing and consent – to allow sending to consumer. Where the subscription template defines anonymisation or pseudo anonymisation, this is applied. Pass events to Send Event Management. Audit everything in the Log.

#### Event Archive

Receive events from Publication and Subscription Engine and archive. Audit everything in the Log.

Receive query from Event Catch-up to find all events in the archive that match query and return them. Audit everything in the Log.

#### Event Catch-up

Receive subscription template from Publication and Subscription Engine. Formulate query and pass to Event Archive. Return all events from Event Archive to Publication and Subscription Engine. Audit everything in the Log.

#### Health Professional Access

Non-Citizen end users – health, social services, local government, commercial companies – web based portal to manually manage aspects of being an event producer, subscriber and consumer. Also used to manually upload producer events and download consumer events.

Network accessible from public sector networks and the Internet.

User authentication from public sector networks and the Internet.

Audit everything in the Log.

#### Log

Store of all audit data. All changes and activities across the service are audited.

#### Analytics

Provide a range of numerical and graphical views on the audit data stored in Log. These will include point in time and trend views in the form of static reports, parameterised reports and dashboards. Provide access to the data to allow analysis by third party tools.

#### Operations Management

Provide operations management of all aspects of the service. Monitoring of availability, performance and error conditions. Alerting on availability, performance or error exceptions. Control of service functions. Backup and restore. Disaster recovery.

The service must be available 24x7 and have the capacity to process and store in the order of 1000 events per second.

# 7 Failsafe Management Service

The Failsafe Management Service implements population tracking and population screening.

It is broken down into the key capabilities shown below:



#### Population Register

Provide a population register that maintains a list of all children (name, identifiers and contact details) that need to be tracked. This will include children (0 – 19 years of age) resident in England, registered with a GP in England or attending a place of education in England.

Allow children to be added, made active, made inactive or removed from the register.

Audit everything in the Log.

#### Health and Wellbeing Plans

Provide each active child on the Population Register with a Health and Wellbeing Plan that defines target dates (points and ranges) for expected observations (e.g. physical developmental examination) and interventions (e.g. vaccination) – termed expected events.

Allow plan to contain prohibited events – events that should never occur.

Allow recording of actuals (termed actual events) against planned observations and interventions.

Allow plans to be added, made active, made inactive, removed or archived.

Audit everything in the Log.

#### Health and Wellbeing Plan Management

Provide management of creation, population and maintenance of Health and Wellbeing Plans.

Create new plan triggered by adding a child to the Population Register. Using the appropriate rules defined in the Rule Base populate expected events in the plan.

Monitor the status of children in the Population Register and synchronise plan status.

Monitor Rule Base for changes and where defined in the rule set apply retrospectively to plans in scope. Note – this would be used for catch-up programmes of vaccination, new interventions, one off public health programme etc.

Audit everything in the Log.

#### Sentinel

Receive event from Child Events Input. Find Health and Wellbeing Plan that the event relates to. If no plan found raise alert.

Record actual event in plan if appropriate.

Check event against expected events and actual events recorded in the plan and appropriate sentinel rules from Rule Base.

Check for duplicate event, early event, late event and prohibited event.

Where action is required, use Child Pathway Status to determine routing of action and use Child Actions Output to send action.

Monitor all Health and Wellbeing Plans using appropriate sentinel rules from Rule Base for missed events and due events.

Where action is required, use Child Pathway Status to determine routing of action and use Child Actions Output to send action.

Record all actions raised and routings in plan.

Audit everything in the Log.

#### Child Events Input

Subscription to the Events Management Digital Service to receive ALL events for every child.

Audit everything in the Log.

#### Child Pathway Status

Provide lookup of current pathway status of child, touch points for services and providers - e.g. primary care provider, social care provider, etc.

Provide contact channels and addresses for providers.

The Sentinel uses these details in conjunction with appropriate rules from Rule Base to decide which services and providers should be sent actions.

Audit everything in the Log.

#### Child Actions Output

Provide multiple I/O channels that allow Sentinel to send actions to external providers. This should include Restful, SOAP, email and file transfer.

Network accessible from public sector networks and the Internet.

End point authentication to public sector networks and the Internet.

Authenticate all interactions and protect all I/O channels from attack vectors.

Audit everything in the Log.

#### Rule Base

Provide a repository of rules that are used by Health and Wellbeing Management to populate and maintain plans, and by Sentinel to determine checks and subsequent actions.

Provide a rules engine to apply rules to input passed via an API and return output.

Audit everything in the Log.

#### Rule Base Management

Provide creating, updating and deleting of individual rules in the Rule Base.

Provide checking of integrity with other rules before committing any changes.

Provide impact assessment (number of Health and Wellbeing Plans affected) before committing any changes.

Provide visual rules designer.

Provide rule set visualiser.

Audit everything in the Log.

#### Health Professional Access

Non-Citizen end users – health, social services, local government – web based portal to view Health and Wellbeing Plans and action history. Also used to manually tailor an individual Health and Wellbeing Plan if required – adding specific expected or prohibited events.

Network accessible from public sector networks and the Internet.

User authentication from public sector networks and the Internet.

Audit everything in the Log.

#### Log

Store of all audit data. All changes and activities across the service are audited.

#### Analytics

Provide a range of numerical and graphical views on the audit data stored in Log. These will include point in time and trend views in the form of static reports, parameterised reports and dashboards. Provide access to the data to allow analysis by third party tools.

#### Operations Management

Provide operations management of all aspects of the service. Monitoring of availability, performance and error conditions. Alerting on availability, performance or error exceptions. Control of service functions. Backup and restore. Disaster recovery.

The service must be available 24x7 and have the capacity to process and store in the order of 1000 events per second and manage 13 million plans.

# 8 Professional Identity Services

A professional can have one or more identities managed by a trusted Identity Provider (IdP). An IdP is trusted if it enforces suitable verification processes that make sure that when a professional applies for an identity they actually are who they say they are.

A professional is deemed to include health and social care professionals.

ePCHR services require the authorisation of individual professionals for request access to view and possibly amend the data managed by an ePCHR. The control of this authorisation will be by the citizen who owns the ePCHR (see Citizen 2 Professional Relationship Service).

There may be a requirement to extend professional identity to specific organisations, e.g. I am happy to allow anyone who works at my GP Practice access to view my ePCHR.

There is **NO** requirement to develop a specific Professional Identity Provider for DCH.

However there is a requirement to make existing Professional Identity Providers (such as CIS) usable by ePCHR services over the Internet using suitable industry standard protocols (for example OpenID etc.).

# 9 Citizen Identity Services

A citizen can have one or more identities managed by a trusted Identity Provider (IdP). An IdP is trusted if it enforces suitable verification processes that make sure that when a citizen applies for an identity they actually are who they say they are.

DCH requires the existence of Citizen Identity Providers as a key enabler for ePCHR providers to identify and authenticate citizen users of their services.

Proprietary IdPs specific to the ePCHR provider is deemed unsuitable as this likely to increase service cost, be more difficult to assess as safe and restrict citizen market choice by making it more difficult to move around different ePCHR suppliers due to lack of standardisation.

There is **NO** requirement to develop a specific Citizen Identity Provider for DCH, but there is a need for at least one (such as GOV.UK Verify) to be operational.

# 10 Citizen 2 Citizen Relationship Services

Multiple citizens with parental responsibility can have access to an ePCHR service for a child. The evidence for parental responsibility may be based on official legal agreements as well as simple claims of kinship or parental rights.

A capability is required to record and manage these relationships at a national level so that it can be assured that appropriate verification processes have been applied.

ePCHR services will need to be able to access it over the Internet to confirm relationships before enabling appropriate access to functionality within their service.

As such this capability can be viewed as an authorisation function.

Proprietary Citizen 2 Citizen Relationships Providers specific to the ePCHR provider is deemed unsuitable as this likely to increase service cost, be more difficult to assess as safe and restrict citizen market choice by making it more difficult to move around different ePCHR suppliers due to lack of standardisation.

Therefore there is a requirement to provide a national service that is capable of managing citizen to citizen relationships. This would include:

* Defining relationship types
* Recording citizen to citizen relationships based on authenticated citizen identities (a relationship assertion)
* Verifying (possibly through a back office process) that relationship assertions are correct
* Allow authorised querying of relationship assertions from the Internet
* Allow removal of relationship assertions

# 11 Citizen 2 Professional Relationship Service

The owner of an ePCHR can allow a professional to have view and/or append access. This access is controlled by the citizen.

A capability is required to record and manage these relationships at a national level so that it can be assured that appropriate verification processes have been applied.

ePCHR services will need to be able to access it over the Internet to define and confirm relationships before enabling appropriate access to functionality within their service.

As such this capability can be viewed as an authorisation function.

Proprietary Citizen 2 Professional Relationships Providers specific to the ePCHR provider is deemed unsuitable as this likely to increase service cost, be more difficult to assess as safe and restrict citizen market choice by making it more difficult to move around different ePCHR suppliers due to lack of standardisation.

Therefore there is a requirement to provide a national service that is capable of managing citizen to professional relationships. This would include:

* Defining relationship types
* Recording citizen to professional relationships based on authenticated citizen and professional identities (a relationship assertion)
* Allow authorised querying of relationship assertions from the Internet
* Allow removal of relationship assertions
* Allow professionals to post a request for access to a citizen
* Allow authorised querying of pending requests by citizen and professional
* Allow citizens to post an invite for access to a professional
* Allow authorised querying of pending invites by citizen and professional

# 12 Electronic Personal Child Health Record

An electronic Personal Child Health Record provides a Child-centric untethered PHR. As such it is an electronic medical record that belongs and is controlled by a citizen. This control includes the ability to add new content from themselves and deciding who to share content with. Because it is untethered the PHR is not controlled or is an extension of an existing health service or organisation system.

A citizen may have multiple concurrent PHRs from private or public providers.

It is broken down into the key capabilities shown below. Note there is NO requirement to provide a national ePCHR. The capabilities are illustrative only and provide context for understanding how the other DCH and enabling national services would interact with an ePCHR.



#### Citizen Identity Providers

A citizen can have one or more identities managed by a trusted Identity Provider (IdP). An IdP is trusted if it enforces suitable verification processes that make sure that when a citizen applies for an identity they actually are who they say they are.

DCH requires the existence of Citizen Identity Providers as a key enabler for ePCHR providers to identify and authenticate citizen users of their services.

Proprietary IdPs specific to the ePCHR provider is deemed unsuitable as this likely to increase service cost, be more difficult to assess as safe and restrict citizen market choice by making it more difficult to move around different ePCHR suppliers due to lack of standardisation.

There is **NO** requirement to develop a specific Citizen Identity Provider for DCH, but there is a need for at least one (such as GOV.UK Verify) to be operational.

#### Professional Identity Providers

A professional can have one or more identities managed by a trusted Identity Provider (IdP). An IdP is trusted if it enforces suitable verification processes that make sure that when a professional applies for an identity they actually are who they say they are.

A professional is deemed to include health and social care professionals.

ePCHR services require the authorisation of individual professionals for request access to view and possibly amend the data managed by an ePCHR. The control of this authorisation will be by the citizen who owns the ePCHR (see Citizen 2 Professional Relationships Providers).

There may be a requirement to extend professional identity to specific organisations, e.g. I am happy to allow anyone who works at my GP Practice access to view my ePCHR.

There is **NO** requirement to develop a specific Professional Identity Provider for DCH.

However there is a requirement to make existing Professional Identity Providers (such as CIS) usable by ePCHR services over the Internet using suitable industry standard protocols (for example OpenID etc.).

#### Citizen 2 Citizen Relationships Provider

Multiple citizens with parental responsibility can have access to an ePCHR service for a child. The evidence for parental responsibility may be based on official legal agreements as well as simple claims of kinship or parental rights.

A capability is required to record and manage these relationships at a national level so that it can be assured that appropriate verification processes have been applied.

ePCHR services will need to be able to access it over the Internet to confirm relationships before enabling appropriate access to functionality within their service.

As such this capability can be viewed as an authorisation function.

Proprietary Citizen 2 Citizen Relationships Providers specific to the ePCHR provider is deemed unsuitable as this likely to increase service cost, be more difficult to assess as safe and restrict citizen market choice by making it more difficult to move around different ePCHR suppliers due to lack of standardisation.

Therefore there is a requirement to provide a national service that is capable of managing citizen to citizen relationships. This would include:

* Defining relationship types
* Recording citizen to citizen relationships based on authenticated citizen identities (a relationship assertion)
* Verifying (possibly through a back office process) that relationship assertions are correct
* Allow authorised querying of relationship assertions from the Internet
* Allow removal of relationship assertions

#### Citizen 2 Professional Relationships Provider

The owner of an ePCHR can allow a professional to have view and/or append access. This access is controlled by the citizen.

A capability is required to record and manage these relationships at a national level so that it can be assured that appropriate verification processes have been applied.

ePCHR services will need to be able to access it over the Internet to define and confirm relationships before enabling appropriate access to functionality within their service.

As such this capability can be viewed as an authorisation function.

Proprietary Citizen 2 Professional Relationships Providers specific to the ePCHR provider is deemed unsuitable as this likely to increase service cost, be more difficult to assess as safe and restrict citizen market choice by making it more difficult to move around different ePCHR suppliers due to lack of standardisation.

Therefore there is a requirement to provide a national service that is capable of managing citizen to professional relationships. This would include:

* Defining relationship types
* Recording citizen to professional relationships based on authenticated citizen and professional identities (a relationship assertion)
* Allow authorised querying of relationship assertions from the Internet
* Allow removal of relationship assertions
* Allow professionals to post a request for access to a citizen
* Allow authorised querying of pending requests by citizen and professional
* Allow citizens to post an invite for access to a professional
* Allow authorised querying of pending invites by citizen and professional

#### Identity and Relationship Broker

To simplify use of Citizen Identity Providers, Professional Identity Providers, Citizen 2 Citizen Relationships Provider and Citizen 2 Professional Relationships Provider; it is deemed desirable to have a national Identity and Relationship Broker that provides a single set of standard and uniform protocols to access these other services through. This broker front end thus decouples access to the individual services making it more flexible and robust than direct access.

Direct access by the ePCHR provider is likely to increase service cost, be more difficult to assess as safe and restrict citizen market choice by making it more difficult to move around different ePCHR suppliers due to lack of standardisation.

#### Repository

A person centred repository of FHIR resources. Resources can be created, read, searched, updated and removed. Sources of resources are; manual input from citizen or health professional (where authorised), manual import by citizen or health professional (where authorised), receipt of events from Child Events Input.

In addition there may be other mechanisms for ingestion of FHIR resources.

The result set of any searches (including all resources in repository) can be exported by citizen or health professional (where authorised).

Audit everything in the Log.

#### Child Events Input

Subscription to the Events Management Digital Service to receive ALL events for child.

Audit everything in the Log.

#### Publication Management

Allows citizen to control the publication of events based on FHIR resources created, updated or deleted from Repository by citizen or health professional.

Audit everything in the Log.

#### Child Events Output

For FHIR resources and operations authorised for publication, send events to Events Management Service.

Audit everything in the Log.

#### Access Management

Allow citizen who is “principal owner” of the PHR to allow and deny operations to other identified citizens and health professionals. Operations could include; read, search, create, update, delete, import and export.

Operations can be scoped to the whole of the repository or specific FHIR resource types.

Access management can be considered an administration operation and could be delegated to other identified citizens and health professionals.

Audit everything in the Log.

#### Authentication and Authorisation

Interface to external identity and authorisation providers.

Audit everything in the Log.

#### Health Professional Access

Non-Citizen end users – health, social services, local government, and commercial companies – web based portal to access the PHR.

May also include App access.

Network accessible from public sector networks and the Internet.

User authentication from public sector networks and the Internet.

Audit everything in the Log.

#### Citizen Access

Citizen end users web based portal and Apps to access PHR.

Network accessible from the Internet.

User authentication from the Internet.

Audit everything in the Log.

#### MVCs

How the contents of the Repository is viewed and used is determined by different functional viewpoint. There will be a range of these functional viewpoints.

Each functional viewpoint can be considered to be a Model-View-Controller (MVC) pattern, where the Model is all or a defined subset of FHIR resources in the Repository.

MVCs should be loosely coupled within the service, enabling new ones to be easily added.

Core MVCs would include:

|  |  |
| --- | --- |
| Basic | |
| Model | All FHIR resources |
| View | Chronological list of all FHIR resources |
| Controller | Create, Update, Delete, Import, Export |

|  |  |
| --- | --- |
| Appointments | |
| Model | All appointment FHIR resources |
| View | Present as a calendar |
| Controller | Cancel, Request, Sync with other calendar apps – outlook, iPhone etc. |

|  |  |
| --- | --- |
| Contacts | |
| Model | All organisation and professional FHIR resources |
| View | Present as a contact book |
| Controller | Search, Browse, Telephone, Email |

Audit everything in the Log.

#### Log

Store of all audit data. All changes and activities across the service are audited.

#### Analytics

Provide a range of numerical and graphical views on the audit data stored in Log.

#### Operations Management

Provide operations management of all aspects of the service. Monitoring of availability, performance and error conditions. Alerting on availability, performance or error exceptions. Control of service functions. Backup and restore. Disaster recovery.

The service must be available 24x7.