The Digital Health & Care Institute (DHI)

The DHI is one of Scotland’s Innovation Centres - funded by the Scottish Government Health & Care Department and the Scottish Funding Council. DHI has spent the last four years (known as DHI Phase 1) facilitating and funding a large portfolio of digital health and care innovation projects that both support health and care service improvement, as well as capitalise on and drive value for Scottish digital industries. During this time, we:

1) Gathered significant evidence and experience as an organisation – informing a view of the digital health and care market, allowing us to see common barriers and opportunities for scale. 
2) Connected with over a thousand innovators, creating an environment to bring diverse capabilities together and developing a mechanism to quickly access these when required. 
3) Developed and then refined a co-design approach with citizens and professionals that could help the community explore and then define the preferred future care models required. 
4) Due to (1) now have an insight into how to align digital health and care capabilities with the new agenda around citizen-centred, co-managed, integrated, and community based care. We can now develop new underpinning digital infrastructure that will help us move from the current, closed nature of data systems to new, open, distributed data systems. Scotland’s care aspirations will not be met if the infrastructure does not evolve to support this. 
5) Developed several digital products that would scale well with the right enablement (see 4), with several of these gaining valuable evidence for commercialisation, and others gaining enough traction to move on to develop the case for change at a national level. 
6) Helped Scottish Government identify issues with the current overall innovation approach, allowing a DHI Phase 2 approach to emerge that was far more systemic and demand driven.

The DHI Phase 2 approach will now:

- prioritise based on national demand drivers to focus activity for the national benefit – with Scottish Government commissioning a small number of core challenges for DHI to address; 
- scope and build whole system service models, clustering relevant technologies, rather than progressing individual technologies – product-focussed pilots are ineffective; 
- incorporate co-design practices to help define the challenges being set and centre-solutions on the citizen; 
- create a risk-free environment to simulate innovative service models, and the digital infrastructure they depend upon; 
- involve the procurement/commissioning community early to ensure that “landing zones” are defined for successful innovations to be adopted and scale up in the health and care system; 
- research both in Scotland and internationally to identify and target specific knowledge gaps such as in regulations and standards; 
- use design approaches to articulate better the real requirements and define “preferable futures” rather than rushing to immediate (and not the right) solutions, and 
- ensure that there is a focus on the skills gap in digital being addressed.
What do you consider have been the main successes of the existing Scottish Government’s eHealth and telecare/telehealth strategies and why?

Linkage of SCI Diabetes to My Diabetes My Way (MDMW) – One of the first developments of its kind globally – this demonstrated how to unify a dataset for a citizen and then develop a set of data driven (and so semi-personalised) tools and educational resources to assist a citizen to self-manage. However, the model now needs to do two things to progress further:

1) **Appreciate complexity** – most notably the likelihood that someone with diabetes may have other health and care needs – which may create interdependencies that a single condition system like this cannot handle, disenfranchising the user. The ability to link this to other data sets to create more nuanced tools would be of great benefit.

2) **Break the tether** – this is still a service built by the NHS, within a clinical / education context. It is an example of a tethered Personal Health Record. While it allows access and even the ability to edit the record by contributing glucose readings – this is limited to one means of communication, using a PC software based uploader. The system is having problems breaking into widespread use because it is not built to be seamless and convenient for citizens who are consuming effortless digital technologies in all other walks of life. If MDMW can evolve to be more open and citizen-led, then there will be a much higher likelihood of adoption at scale. As will be noted later in this paper, MDMW should not have to build bespoke infrastructure to offer this openness and interoperability – instead some common, open and distributed infrastructure could be developed to help MDMW and other services that may emerge to do so quickly, cheaply and consistently.

Clinical Portal – this is a virtual electronic patient record that draws from existing patient record databases into one view, rather than centralising to create a national database. ‘Single sign on’ allows for seamless access to these disparate sources of information where previously a clinician would need to sign into multiple services simultaneously. This development aligns well with progressive approaches to data sharing and integration – it works on the principle of ‘using what you have’ in terms of existing infrastructure, and the principle of reuse of data / drawing from local databases rather than trying to centralise the stored data. However, note that this works best for clinical / service oriented requirements – the same ‘single sign on’, centralised approach cannot be easily applied to more diverse and personalised citizen facing services.

Creation of the DHI – the Scottish health and care community anticipated the emergence of the digital health and care market long before it accelerated to the scale it enjoys today. DHI was created by this community to act as a force that drives digital health and care progress forwards, breaking new ground and leveraging Scotland’s broader capabilities to help health and care services transform. The ‘arms-length’ nature of the DHI as an Innovation Centre allows for scrutiny and critique (such as found in these papers) which help Scotland remain progressive in its approach to digital health and care.
What do you consider have been the main failures of the existing Scottish Government’s eHealth and telecare/telehealth strategies and why?

- **Tensions between Operations and Innovation** - The eHealth Leads in Scotland have operational responsibility for maintaining a complex set of legacy systems that are increasingly taxed to deliver new or enlarged services they were not designed to satisfy. The strategies and development work around digital health and care place an unrealistic demand on this group to lead and progress next generation digital infrastructure, when they are barely resourced to maintain the status quo.

- **Guidance only goes so far** - While the eHealth community in Scotland cooperates strategically, benchmarks and enjoys some economies of scale, the health boards in Scotland are still fundamentally separate organisations and Scottish Government only acts as a guide and facilitator. This in turn means that the culture around data sharing has remained focused on point to point data sharing agreements and integrations between health boards. Some development have occurred across boards – such as the Emergency Care Summary or Key Information Summary. However, other governments have mandated and resourced more comprehensive common data exchange and integration approaches that have allowed them to accelerate beyond Scotland when it comes to realising the benefits of broader data sharing.

- **No recurrent funding for new developments** – a common problem across all digital development activities is that the funding is almost always only seed funding for initial proof of concept. In a best-case scenario, the new development proves successful. This then usually results in an already strained health board eHealth budget being required to stretch to cover the ongoing costs of the new digital capabilities. Often this cannot be achieved and new developments cease when the project funding finishes.

- **Decisions to invest** – There is no cohesive framework for how Scotland invests in new digital health and care services:
  - Due to the emerging nature of many of the digital capabilities, there is no easy way of benchmarking value – and so no one can clearly say what ‘good’ looks like.
  - There is an unrealistic expectation around the burden of proof for digital service investment – often requiring favourable cost / benefit in the short term as well as advanced levels of evidence around clinical outcomes and technical viability.
  - This misunderstands that these developments are not new ‘treatments’, but a new way of offering services – and that developments of this nature will require several iterations to get the service right, and it will only yield the required benefits if the service is scaled up and other non-digital services are decommissioned as a result.
  - This is linked to the issue of nonrecurrent funding for new developments. A pilot is really just deferral of a decision to invest. Instead we need to commit to a new way of working, plan for a phased development that iterates and replaces non-digital capabilities, and that has recurrent funding built in.
  - The first couple of years of a scaled digital service are unlikely to yield benefits, this must be planned for an improved upon as necessary until new ground is broken and the delivery channels are shifted.

- **Building for services, not designing for citizens** – While more recently there have been more efforts to design services with citizens, there is a still a default to building to improve clinical workflow and support service delivery. This is understandable given the successes achieved in this manner in the past. However, this has led to approaches that centralise and standardise
interfaces and in general, apply thinking that has led to good gains for clinical users – but that are not necessarily engaging or intuitive for citizens.

- **Engaging SMEs** – the eHealth objective to engage better with Scottish SMEs is admirable but difficult to achieve in practice. DHI’s experiences trying to broker these relationships highlight that most SMEs simply can’t operate to the scale or deal with the rigour and governance required by eHealth development. Equally the public sector is still only just beginning to understand developmental procurement processes, and still has a hard time managing risk associated with smaller supplier relationships. There is no easy answer here. It will be damaging to retain this strategic objective if it continues to be a token commitment only.

How well does the Scottish Government’s draft Digital Health and Social Care Vision 2017-2022 address the future requirements of the NHS and social care sector?

&

Do you think there are any significant omissions in the Scottish Government’s draft Digital Health and Social Care vision 2017-2022.

The draft vision is not definitive or strong enough in its wording – it has to address the core barriers and opportunities around data sharing to support real progress over the coming years. Please see the table below for comment.
As a citizen of Scotland:

<table>
<thead>
<tr>
<th>Vision Statement</th>
<th>Comment</th>
<th>Alternative</th>
</tr>
</thead>
</table>
| I have access to the digital information, tools and services I need to help maintain and improve my health and wellbeing. | • This statement could be read very superficially and arguably NHS Inform already satisfies this aspiration.  
• A distinction should be made between access to generic information / tools vs access to your own records, treatment options, care plan and tools that leverage this data to offer personalised self-management options.  
• Access to information alone will not bring about significant improvements. A citizen should be able to both act on the information and contribute information into the record in turn.  
• If this is only delivered through state provided digital services in a ‘Once for Scotland’ approach, this will not offer the choice and personalisation required. | I can use widely available digital tools and services to manage my own health and wellbeing, knowing that these tools can use and contribute to my personal and official health and care records. |
| I expect my health and social care information to be captured electronically, integrated and shared securely to assist service staff and carers that need to see it, | • Capturing the information electronically could mean scanning letters and storing them as PDFs. It doesn’t also make a commitment to ease of use and reduction in duplication.  
• The information is already being integrated – but saying how matters. The current approach is very onerous and based on point to point integration and data sharing agreements between organisations that can take two or more years to put in place or change. There are other ways of doing this.  
• This doesn’t link into the broader digital public services agenda.  
• There is no mention of data ownership or consent. Nor does it offer transparency around data use for the citizen. There is an opportunity here to make a stronger statement to keep Scotland progressing in line with leading European approaches. | I expect my health and care information to be captured once only, and for this information to be made available to all relevant public services, and for any use of this information to be known to me and based on my consent. |
| and that digital technology and data will be used appropriately and innovatively to help plan and improve services, enable research and economic development | • Again, this happens today. It is not clear how this statement can drive change of any scale or ambition. Also, from a citizen’s point of view is this important? | I expect to be able to consent to the use of my health and care information to support improvements in public services while also creating a market for the digital tools I need. |
What key opportunities exist for the use of technology in health and social care over the next 10 years?

The answer to this question is intricately linked to the need to share information more effectively – the answer to both questions is summarised below. For more detail please see the accompanying paper “Advancing Digital Health & Care: Exploring the infrastructure required for citizen-centred services”.

What actions are needed to improve the accessibility and sharing of the electronic patient record?

To answer this question the DHI proposes to first answer a more fundamental one: Why is data not shared more consistently for more effective and accessible digital public services?

The UK is ranked highly (6th) for digital progress overall, but relatively poorly (19th) for accessibility and use of digital public services. This pattern extends to digital health and care services. Note there are no rankings for Scotland separately and so it is assumed that Scotland broadly follows the rest of the UK – with solid digital progress that doesn’t necessarily translate into easily accessible digital public services.

In the UK, like many European countries, there are successful infrastructures that have improved service delivery from a systems perspective – such as Electronic Health Records (EHRs) and Clinical Portals. These worked very well in a system in which the NHS was expected to control the dialogue and optimise clinical outcomes for citizens. As care is shifted towards more distributed, citizen-centred, and community based models, these systems – which are largely centralised - can no longer handle the complexity and diversity involved in integrated and personalised care.

Health and care systems have attempted to remedy this through ‘Patient Portal’ platforms by giving citizens access to their EHR and by digitising transactions such as appointment and repeat prescription booking. This has had some positive impact from an administrative and workflow point of view but has as yet shown very poor uptake and retention of use and has shown no improvements in health outcomes for citizens. This is largely because this approach reflects only small changes within the existing patriarchal model of healthcare system and medical control, offering citizens only a small access point into the healthcare system as it already exists, rather than meaningful co-management functionality.

To learn from those countries topping the European digital public services accessibility and use rankings – Finland and Estonia – they have more radical approaches to citizen empowerment. Thinking holistically and with citizen access and empowerment in mind, these countries share common components around national identification, enforced database interoperability and consent driven, transparent control of data flows by the citizen. This simplifies access and builds trust in data sharing, which in turn creates a more seamless citizen experience. They are both also developing genuinely personally held data capabilities that can adjoin the statutory record to personalise services more effectively. This approach is based on a national dialogue led at the highest levels politically and organisationally.
Scotland currently has taken a more cautious route. The forcefulness of the mandated change around identity, privacy, citizen control and data sharing is difficult to commit to politically, and the benefits of doing so are not necessarily clear.

To close the gap between Scotland and the European leaders, it is recommended that, at a minimum there is a national dialogue initiated around a Scottish e-society – focusing on effective delivery of citizen centred digital public services and therefore concerning identity, privacy and transparency in the context of effective public service provision. Currently development is moving slowly because the public sector does not have a clear mandate from its citizens to transform services.

It is crucial to note that this is not a debate about national identity schemes and whether we follow the more extreme example set by the European leaders. However, there are a number of principles that have significantly empowered citizens in these countries that we must learn from.

Realistic Medicine, as espoused by the Chief Medical Officer, can be achieved by enhancing our ability to share data in a consent driven fashion, allowing more seamless and personalised services, with diversity for citizen but built on a consistent core infrastructure and standards base. Key to this are three interlinked concepts:

1) If the citizen is to be empowered, then they must own their own data, must see the data held by others about them and must be able to limit how data is shared effortlessly and directly.
2) Care is distributed – so the digital infrastructure must not centralise power and access. If citizens feel they genuinely have this control and choice, then trust in the system increases and data begins to flow more effectively.
3) Personalisation is more than just customisation of generic services - permission-less innovation must flourish near the citizen, but within a governed set of standards and norms to protect quality of care.

A distributed care system supported by a distributed, but standards based digital infrastructure, is exactly what the Scottish digital health and care marketplace needs to flourish. The leading e-societies of Europe are now capitalising economically on their open, distributed, data rich systems. Businesses are able to add value significantly quicker with far fewer barriers, and can demonstrate benefits directly to citizens. This in turn then allows them to engage with global markets that are increasingly working to the same consumer focused, distributed delivery models.

So, in conclusion, it is recommended that Scotland begins with citizen-centred co-design activity to understand how to empower citizens in a digital era and then build a distributed digital infrastructure that can then allow innovation to flourish in response to these diverse needs.

DHI can provide materials on request that highlights:

1) More detail of the leading approaches in Europe.
2) Case studies from co-design activity with Scottish citizens demonstrating their interest and need for this type of ownership and empowerment around data sharing.
3) Tangible next steps that could be taken to gently begin a broader dialogue around citizen empowerment and data sharing.
What are the barriers to innovation in health and social care?

There are multiple barriers – but DHI identifies the data sharing issues raised above as the most significant by far. Additional comments:

- Digital innovation is largely regarded as a pre-commercial procurement activity that depends on the initiative and energy of a small number of individual enthusiasts, rather than a strategic activity require to keep services sustainable.
- Key decisions need to be made about the system level change required for sustainability of public services. From this, new digital services need to be created and acknowledged as the ‘new normal’ – not asked to justify benefits in isolation as discrete projects.
Advancing Digital Health & Care

Exploring the infrastructure required for citizen-centred services

Chaloner Chute, Chief Technology Officer, the Digital Health & Care Institute
# Contents

1. Executive Summary .................................................................................................................. 3
2. European Digital Progress ........................................................................................................ 5
3. European Digital Health & Care (eHealth) Progress ................................................................. 6
4. Analysis ......................................................................................................................................... 8
   4.1. General eHealth Features ...................................................................................................... 8
      4.1.1. Existing eHealth Services .............................................................................................. 8
      4.1.2. Emergence of the Person Held Record ........................................................................... 9
   4.2. Lessons from the most accessible eHealth services .............................................................. 10
      4.2.1. Case Study 1: Finland .................................................................................................... 10
      4.2.2. Case Study 2: Estonia .................................................................................................. 12
      4.2.3. Discussion .................................................................................................................... 14
   4.3. Broader eGovernment Development for Future Care Integration ........................................ 18
5. Implications for Scotland ........................................................................................................... 20
      5.1.1. Identity & Data Sharing ................................................................................................. 20
      5.1.2. The Personal Health Record ......................................................................................... 22
      5.1.3. Case Study – A Personal Data Store for people with Multiple Sclerosis (MS) ........... 25
   5.2. Recommendations for Strategy Going Forward ................................................................. 26
   5.3. Conclusion ............................................................................................................................ 28
6. References ................................................................................................................................... 29
1. Executive Summary

The use of digital technology is advancing rapidly across Europe with many citizen’s including those thought to be ill equipped or excluded now accessing public services online. The UK is ranked highly (6th) for digital progress overall, but relatively poorly (19th) for accessibility and use of digital public services.

This pattern extends to digital health and care services. In the UK, like many European countries, there are successful infrastructures that have improved service delivery from a systems perspective – such as Electronic Health Records (EHRs) and Clinical Portals. These worked very well in a system in which the NHS was expected to control the dialogue and optimise clinical outcomes for citizens. As care is shifted towards more distributed, citizen-centred, and community based models, these systems – which are largely centralised - can no longer handle the complexity and diversity involved in integrated and personalised care.

Health and care systems have attempted to remedy this through ‘Patient Portal’ platforms by giving citizens access to their EHR and by digitising transactions such as appointment and repeat prescription booking. This has had some positive impact from an administrative and workflow point of view but has as yet shown very poor uptake and retention of use and has shown no improvements in health outcomes for citizens. This is largely because this approach reflects only small changes within the existing patriarchal model of healthcare system and medical control, offering citizens only a small access point into the healthcare system as it already exists, rather than meaningful co-management functionality.

To learn from those countries topping the European digital public services accessibility and use rankings – Finland and Estonia – they have more radical approaches to citizen empowerment. Thinking holistically and with citizen access and empowerment in mind, these countries share common components around national identification, enforced database interoperability and consent driven, transparent control of data flows by the citizen. This simplifies access and builds trust in data sharing, which in turn creates a more seamless citizen experience. They are both also developing genuinely personally held data capabilities that can adjoin the statutory record to personalise services more effectively. This approach is based on a national dialogue led at the highest levels politically and organisationally.

Scotland currently has taken a more cautious route. The forcefulness of the mandated change around identity, privacy, citizen control and data sharing is difficult to commit to politically, and the benefits of doing so are not necessarily clear.

To close the gap between Scotland and the European leaders, it is recommended that, at a minimum there is a national dialogue initiated around a Scottish e-society – focusing on effective delivery of citizen centred digital public services and therefore concerning identity, privacy and transparency in the context of effective public service provision. Currently development is moving slowly because the public sector does not have a clear mandate from its citizens to transform services.
Realistic Medicine, as espoused by the Chief Medical Officer, can be achieved by enhancing our ability to share data in a consent driven fashion, allowing more seamless and personalised services, with diversity for citizen but built on a consistent core infrastructure and standards base. Key to this are three interlinked concepts:

1) If the citizen is to be empowered, then they must own their own data, must see the data held by others about them and must be able to limit how data is shared effortlessly and directly.

2) Care is distributed – so the digital infrastructure must not centralise power and access. If citizens feel they genuinely have this control and choice, then trust in the system increases and data begins to flow more effectively.

3) Personalisation is more than just customisation of generic services - permission-less innovation must flourish near the citizen, but within a governed set of standards and norms to protect quality of care.

A distributed care system supported by a distributed, but standards based digital infrastructure, is exactly what the Scottish digital health and care marketplace needs to flourish. The leading e-societies of Europe are now capitalising economically on their open, distributed, data rich systems. Businesses are able to add value significantly quicker with far fewer barriers, and can demonstrate benefits directly to citizens. This in turn then allows them to engage with global markets that are increasingly working to the same consumer focused, distributed delivery models.

So, in conclusion, it is recommended that Scotland begins with citizen-centred co-design activity to understand how to empower citizens in a digital era and then build a distributed digital infrastructure that can then allow innovation to flourish in response to these diverse needs.
2. European Digital Progress

Europe’s Digital Progress Report (European Commission, 2017) identifies a rapid uptake of digital channels in the communication between citizens and public services. There has also been a decrease in digital exclusion as private and public services develop methods of improving access. Internet use for elderly people has also expanded greatly in this five-year period (48% to 65% of the population).

Figure 1: Preferred channel for submitting forms to public authorities by EU citizens

Looking then to comparative indicators, the UK is placed sixth for overall digital progress in Europe.

Figure 2: Digital Economy & Society Index

However, the UK only ranks 19th when looking at only the use of digital public services.

Figure 3: European Digital Public Services Dimension

1 The Digital Public Services dimension indicators: 1) % internet users who have completed an online public service form, 2) how much the form is pre-filled from existing public service data, 3) how many interactions can be performed completely online, 4) the government’s commitment to open data.
3. European Digital Health & Care (eHealth) Progress

Deployment & Adoption by Services

The UK is acknowledged to have good foundation eHealth infrastructure, ranking sixth in the European benchmarking exercises for deployment of eHealth services in hospitals, and seventh for primary care.

Figure 4: Benchmarking Deployment of Hospital eHealth Services (Maghiros & Sabes-Figuera, 2013)

![Benchmarking Deployment of Hospital eHealth Services](image1)

Figure 5: European Index of Primary Care eHealth Adoption (European Commission, 2013)

![European Index of Primary Care eHealth Adoption](image2)
Availability & Use

However, the UK does not perform as well, ranking 20th, when assessing how this eHealth infrastructure then translates into the use of digital services by staff and citizens (such as embedded clinical decision support, electronic communication with patients, and remote monitoring of patients).

Figure 6: Benchmarking Deployment of Hospital eHealth Services 2012 – Availability & Use (Maghiros & Sabes-Figuera, 2013)²

This paper will explore the disparity between the UK’s robust eGovernment and eHealth infrastructure and the relatively poor accessibility and use of digital services provided on top of that infrastructure.

Note that no separate data is readily available that compares Scotland with the rest of Europe in these terms. It is assumed for the discussion that follows that Scotland is broadly representative of the UK experience as a whole – that Scotland has great digital progress overall, but that it has struggled to capitalise on this through usable and accessible digital public services.

² Note the equivalent data was not available for availability and use in primary care.
4. Analysis

This section first outlines the common eHealth approaches across most European countries. It then goes on to contrast this with the emerging approaches that distinguish the countries leading in terms of accessibility and usability of these services. It finishes with a discussion of the broader requirements for eGovernment as health and care services integrate.

4.1. General eHealth Features

4.1.1. Existing eHealth Services

Besides basic ICT information and infrastructures, the key pillars of eHealth include (European Commission, 2013):

1) **Electronic Health Record (EHR)** - “Systems used by healthcare professionals to enter, store, view, and manage patient health and administrative information and data” – characterised by a spread of different, disconnected systems in primary, secondary and social care.

2) **Health Information Exchange (HIE)** - “The process of electronically transferring / sharing / enabling access to patient health information and data.” - characterised by:
   - **Point to Point Integration** - and data sharing between health and care providers, governed by information sharing agreements.
   - **Clinical Portals** – provides a web interface that draws together many disparate sources of patient information into one, usually read-only, view.

3) **TeleHealth** - “The use of broadband-based technological platforms for providing health services, medical training and health education over a distance.” - characterised by:
   - **Remote consultation** - replacing face-to-face with video conference or secure messaging.
   - **Remote monitoring** – either diagnostic or trend monitoring – most commonly for blood pressure and blood glucose control.
   - **Training and education** – using mainly video conferencing technology.

4) **(Tethered) Personal Health Record (PHR)** - “Electronic systems allowing patients to have secure access to, and manage, their health information.” - characterised by:
   - **GP Patient Portals** – that offer patients a read-only view of the Electronic Health Record (EHR) held by GPs on a practice by practice basis.
   - **National Patient Portals** – that draw information from across multiple health and care systems to offer a single web-based view of the citizen’s record and transactional services.
   - **Condition Based Patient Portals** – that offer patients a web-based view of pertinent information about their condition – usually a long-term condition such as diabetes.
4.1.2. Emergence of the Person Held Record

Due to the emerging nature of the Person Held Record / Personal Health Record (PHR), it is often confused or defined in overlapping terms with a Patient Portal, or Electronic Health Record (EHR):

- A “tethered” PHR is a means by which citizens can view the data held by a health and care system (EHR). This is often offered in the context of a Patient Portal offering secure login and collocating this information with educational resources and some transactional services such as appointment booking. The tethered PHR can sometimes allow for basic editing of demographic data by the citizen, or at least feedback on changes and errors.
- An ‘untethered’ PHR is an entirely citizen-controlled and edited data repository. Use of the data within it is driven by a consent model, ensuring that privacy is maintained (satisfying new General Data Protection Regulations (GDPR) for active consent to share data).

The ‘tethered’ PHR / Patient Portal concept has been discussed since the early 2000s and has now evolved to include transactional elements such as appointment or repeat prescription booking. It is important to understand what drives the uptake of tethered PHRs and Patient Portals globally. The patient portal concept is intended and often narrated to be a tool to empower a citizen and increase the ease with which they access services.

However, the main drive and uptake of this technology is found in the U.S. In 2009, the U.S. Congress passed the HITECH Act, which authorised incentive payments to physicians who demonstrated “meaningful use” of Patient Portals. Since 2015 those not adhering to this face penalties. Meaningful use at stage 1 required 5% of service users to register for and use a Patient Portal. Many practices have struggled to hit even this seemingly low level of adoption. Figure 7 below highlights some of the reasons for poor uptake.

**Figure 7 – Main reasons for poor uptake of a patient portal (Softwareadvice.com, 2014)**

These are the hallmarks of a system built for the service provider, not the user. The critique most often levelled is that the platforms are developed with a ‘build it and they will come’ mentality, focusing on satisfying the ‘meaningful use’ criteria and building to achieve transaction-based administrative savings for the practices, rather than focusing on value to the patient.
An unnamed patient portal vendor’s sales documentation captures this well:

“Beyond basic requirements of sharing health record information, portals should be a place for each provider to customize the patient interaction based on their specific practice needs and workflow.”

Outside of the U.S. some countries have adopted national patient portals, portals for individual conditions or patient groups, or practice-based portals at a local level. In most cases the value is the ability to channel shift people away from offline communication channels, reducing the service pressure and administrative burden on staff, with parallel benefits projected for patient empowerment and therefore improved outcomes.

However, despite some evidence to suggest some efficiency and administrative savings, actual adoption by patients remains very low. Global reviews have also found no evidence to substantiate the view that empowerment and improved outcomes follow Patient Portal implementation (Ammenwerth, Schnell-Inderst, & Hoerbst, 2012).

The key question is, are we perpetuating and forcing an industry-led service offering that citizens simply haven’t asked for? There is clear evidence that people want access to their records and want to book appointments and prescriptions online (Accenture Consulting, 2016). What isn’t clear is that citizens gain value from systems that are built predominantly to satisfy the transactional needs of health and care providers.

Patient Portals have a place in a broader digital health and care infrastructure, but the transactional efficiencies they bring should be the focus, with other elements of the infrastructure being developed to support a package of capability that can empower a citizen and improve their outcomes. Development must include untethered PHR functions that are built on the citizen’s terms, allowing them to co-manage their own care, rather than purely focusing on the Patient Portal functionality to involve citizens in the service oriented clinical and administrative workflow.

### 4.2. Lessons from the most accessible eHealth services

Estonia and Finland rank first and second in Europe for both overall digital public services and for the availability and use of eHealth services. The Estonian composite indicator for eHealth availability and use is double the EU average and triple that of the UK. This section explores the approach to broader digital public service delivery that enables such high levels of access and use.

#### 4.2.1. Case Study 1: Finland

**A National Personal Health Record**

Kanta Services is the Finnish National Archive for healthcare information. They are now introducing an untethered Personal Health Record (PHR) that will enable citizens to enter their own health-related data (Hypponen, 2017). Third parties will be able to develop digital services and apps for citizens that
produce, store and analyse this personal data. Health and social care professionals will be able to access the data only with the citizen’s active consent.

Sandbox development environments are currently available for early stage experimentation and development. The following elements are being developed to help govern this capability:

- Consent management standards and systems
- Authorisation and data security solutions
- Broader technical standards around identity, authentication and data sharing
- Certification criteria and process for PHR linked apps
- Legislation to allow, through consent-driven processes, for these apps to access official health and care data held in the main electronic health record.

Capitalising on this Infrastructure

The Finnish Digital Primary Care (ODA) project is a new approach to digital citizen monitoring, symptom checking and self-management. It builds upon this new Finnish National PHR approach. It is predicated on a digital-first approach to taking a person’s own data (Untethered Personally Held Record or PHR), combining it with the data from their Electronic Health Record or EHR and then using automated decision support systems to help them self-manage, make decisions and interact further with services if required.

This integration of records enables a citizen’s own data to auto-populate many of the data fields in the tool – significantly cutting down on the time and effort spent, while ensuring advice and self-management options are given in a personalised manner. This in turn then forms the first step in a dialogue with the health and care system, rather than a mere disconnected symptom check.

Technological Foundations

Sitra, the Finnish innovation fund, states that for the diverse provision and use of digital services such as this, there is a requirement for “the electronic identification of citizens and the exchange of information between databases in a unified manner. The existing databases of public organisations could be exploited for service production purposes, through the use of a common data exchange layer. Several types of registration data, such as health records or motor vehicle registrations, would only need to be stored in one place – the layer would enable the use of original, up-to-date data from its original source when, and where, needed. Together with an eID this also enables citizens to check and update their own data and to use a variety of public and private services online. A data exchange layer operates on the basis of standardised interfaces between information systems.” (Sitra, 2017) (emphasis added).

Cultural and Political Foundations

However, technological elements are only one aspect of the fully transparent, interoperable digital infrastructures required for the development of effective digital self-management services. The following are the broader key features required for effective eGovernment, as it relates to the Finnish experience (Korhonen, 2016):

- A culture of openness – that values transparency in the delivery of eGovernment and ensures broad-based support for transparent and effective data sharing. This includes a national
dialogue in which everyone understands that owning your own digital identity enables this enhanced transparency and control on the part of a citizen.

- **High level leadership** - The Prime Minister chairs the Finnish Information Society Programme.
- **Legislation compatible with digital government** – acts that promote and ensure the secure and effective interoperability of information systems, electronic identification as standard, and openness of access to non-personal data while protecting personal data.
- **Proper base registers form the foundation** – population, company, property and other registers are core infrastructure for eGovernment and must hold comprehensive, accurate and up to date information, and protect against unauthorised changes.
- **Interoperability and cooperation within government** - Interoperability within government is a prerequisite for sophisticated e-service provision. Today, internet technologies dominate and typical technical interoperability problems can be solved quite easily. In the Finnish administration, the Achilles heel of interconnection between different systems usually lies at higher levels of interoperability. In some cases it is about semantics. The same concepts, sometime even simple ones, such as addresses and names, can have slightly different meanings and formats. In other cases, strict legislation may prevent the exchange of data between organisations. The Finnish government is continuously working on these issues to overcome the obstacles for smooth interoperability. If there is no proper interoperability, then there are no seamless digital services either.
- **Focus on the citizen** - Customers’ needs should be the main focus in service design. Digital services are not just forms on web pages and you should not rush to modify existing services to electronic ones. Some procedures (or services) might not be needed at all – either in traditional or electronic format.

4.2.2. Case Study 2: Estonia

**A Distributed, transparent eHealth model**

A legislative programme was developed that enforces the following foundation principles:

- All health and care providers must send data to the Health Information System (HIS).
- Access given only to licensed professionals and others permitted by law.
- ID card for authentication and digital signature.
- The citizen has the right to close their own data on the central database (opt out), access their own data (Patient Portal), declare their intentions and preferences and monitor who visits and undertakes activities with their data on the HIS – all actions leave a secure, permanent trail.

**Capitalising on this Infrastructure**

The Electronic Health Record is a nationwide system that integrates data from Estonia’s different healthcare providers to create a common record for each patient. Using the data exchange layer, X-Road, the EHR retrieves information from various systems, and presents it in a standard format. In an emergency situation a doctor can use a patient’s ID card to read time-critical information such as blood
type, allergies, recent treatments, ongoing medication, or pregnancy. The system also compiles data for national statistics, so the relevant ministry can measure health trends, track epidemics, and make sure that its health resources are being spent wisely.

Patients have access to their own records, as well as those of their children. By logging into the Patient Portal with an electronic ID Card, the patient can review their past doctor visits and current prescriptions, control which doctors have access to their files, and even receive general health advice.

**Technological Foundations (E-Estonia, 2017)**

X-Road is the backbone of e-Estonia. X-Road is an integration layer that allows all public (and some private) databases to interact, making integrated digital services possible. Institutions are not locked into any one type of database or software provider. Databases are decentralised – every government agency or business can choose the software/hardware product that is right for them. All of the Estonian e-solutions that use multiple databases use X-Road. All outgoing data from the X-road is digitally signed and encrypted. All incoming data is authenticated and logged. National ID cards are mandatory in Estonia, giving digital access to all of Estonia’s secure digital services. The embedded chip on the card uses 2048-bit public key encryption, making it a secure and definitive proof of ID in an e-environment. The ID card is regularly used in Estonia, e.g.:

- As a national ID card for legal travel within the EU for Estonian citizens
- As the national health insurance card
- As proof of identification when logging into bank accounts from a home computer
- For digital signatures
- For online voting
- For accessing government databases to check one’s medical records, file taxes, etc.
- For picking up e-Prescriptions

The six main security principles of the Estonian eHealth system are:

- Secure authentication - of all users with ID-card or mobile ID.
- Digital signing or stamping - of all health documents.
- Maximum transparency and accountability – actions will leave an unchangeable, secure trail.
- Cording of personal data – separating personal data from medical data.
- Encrypted database – that removes the confidentiality risks.
- Monitoring – of all actions together with corresponding counter-measures.

**Cultural and Political Foundations (the Estonian Information Society Strategy)**

The Estonian Information Society Strategy is built on the following foundations:

- the development of the information society in Estonia is a strategic choice with public sector leading a partnership with the private and third sectors;
- the public sector is a smart customer, ensuring that in public procurements there is as much freedom as possible for innovative solutions;
- the information society is created for all Estonian residents, although particular attention is paid to the integration of social groups with special needs;
• the information society must not undermine people’s sense of security. The protection of basic rights, personal data and identity must be ensured, and mitigation of non-acceptable risks in information systems must be guaranteed;
• citizens will have increasing control over the use of their personal data;
• the public sector employs the already existing technological solutions (i.e. the ID card, the data exchange layer X-Road) and avoids duplication of IT solutions;
• the public sector re-organises its business processes so as to ensure a one-off collection of data from citizens, entrepreneurs and public bodies;
• the public sector gives equal treatment to different hardware and software platforms and ensures interoperability of information systems by using open standards;
• the collection of data and the development of ICT solutions proceed from the principles of re-usability.

Some Dos and Don’ts based on Estonia’s experience:
• Do – Create a decentralised, distributed system so that all existing components can be linked and new ones can be added, no matter what platform they use
• Don’t – Try to force everyone to use a centralized database or system, which won’t meet their needs and will be seen as a burden rather than a benefit
• Do – Be a smart purchaser, buying the most appropriate systems developed by the private sector
• Don’t – Waste millions contracting large, slow development projects that result in inflexible systems
• Do – Find systems that are already working, allowing for faster implementation
• Don’t – Rely on pie-in-the-sky solutions that take time to develop and may not work

4.2.3. Discussion

There are common features adopted by the European countries leading on both the development of digital public services and the availability and use of eHealth services, from which lessons can be learned. These include a commitment to:

1) Think beyond health and care - Common needs and use cases for a citizen’s data already exist across the broader public service estate. Investment in health and care specific digital infrastructures and services will duplicate effort and limit the full power of data driven e-governance. A citizen’s health is very often intimately linked to transport, education, welfare, housing, etc. – and so should not be serviced in a silo.

2) Distribute services – all sectors are experiencing a distribution of information and capability as digital technologies democratise processes. Health and care is shifting into community settings and aspires to put the citizen at the centre. This requires a shift in mindset around how digital infrastructure is developed – it cannot be centralised if it is to meet these needs.
3) Partner with, don’t just procure from, industry – Industry are adept at designing for the customer. The entrepreneurial thought process demands that customer needs be met locally, and a marketplace can offer the choice that would be extremely onerous and costly for the public sector to provide centrally. Importantly, citizens may expect to engage through mediums they already use – almost always provided by commercial companies. Interoperating with these capabilities will drive much greater adoption than building bespoke solutions and attempting to enforce use at great cost. This is linked to the need to distribute information and services to meet citizen needs flexibly. If the state attempts to provide centralised services through large scale ICT projects, this then reduces the opportunities to personalise and democratise access to care while also damaging the country’s ability to derive the local economic benefit (which requires an open marketplace based on standards).

4) Centre design on the citizen:

a) Avoid enforcing centralised interfaces - Patient Portal and equivalent technologies tend to be developed for services rather than service users. This is also linked to the need to distribute services and use what already exists. Avoid forcing a citizen to interact with one centralised interface where possible.

b) Avoid digitising existing paper processes – the chances are that digital tools could enable a completely different way of working, or remove the need for an interaction in the first place.

c) Instead understand attitudes to data sharing and use - engage in research around the acceptability of modern digital systems and their requirements – such as identity, consent and privacy. Once this is understood, services can be developed that meet needs for service, but also for security and privacy.

5) Develop a common approach to identity

a) National ID Card – this evocative notion has been resisted in the past in many countries. It conjures up fears for privacy and an overreaching ‘nanny state’.

b) We already have several IDs – There are identification numbers – such as the NHS CHI number, national insurance numbers, etc. The citizen does not ‘own’ these numbers at present – they are seen only as a means for the state to store and recall information on a citizen. There are also entitlement cards such as YoungScot and the National Entitlement Card (NEC). These numbers and cards have not been unified but the data sets behind them are already easily linked.

c) Citizens cede much more privacy to businesses – such as Facebook and Google – often without knowledge or any transparency.

d) A common identity can enhance ownership and transparency – in both Finland and Estonia, strict governance applies, with citizens now able to see who is using their data and query it. Citizens can withdraw their data from use or consent to its use by others. This is significantly better than public services exchanging and linking data sets behind the scenes from a privacy and transparency point of view – but this only works with a citizen owning their national ID.

e) Develop in dialogue – as per the citizen-centred point, co-design can help identify the right balance and acceptable use cases and structures for identity in the context of
consent, citizen empowerment and new service development. It is clear that this level of identification will only be acceptable with a significant increase in control and transparency of the data that links to it.

6) Develop a data exchange layer

a) Create data once and then reuse it - Critical to the citizen’s perception of seamless integrated care is the ability to only tell their story once, and for everyone to work to that story and keep up to date as it evolves. The Estonian Exchange Layer was estimated to have saved 7,182,262 working hours last year.

b) This interconnectedness is one of the critical measures for the European measures of accessibility and use of eHealth. However, “the use of inter-connected registers with the purpose of avoiding re-submission of data by the user is not yet widespread. Pre-filled forms are available, for half of EU countries, for less than half of the cases where this could be possible, and sometimes much less than that. Some notable exceptions are Malta, Estonia and Finland, with seven other countries following suit.” (European Commission, 2017).

Figure 8: Use of interconnected registers to auto-populate forms

The UK is third from the bottom on this particular measure.

c) Use open standards and build for interoperability – to take advantage of existing capabilities. Do not build bespoke infrastructure and avoid proprietary ecosystems.

d) Exchange Layer - Both (a) and (b) have been achieved in Estonia and Finland with the creation of a Data Exchange Layer. This is an open, secure and standards-based intermediary layer that all public service databases can connect to. It does not store data centrally or create new databases – instead it allows different databases to be called on to a portal for a unified view by the citizen’s data, and in turn to be shared with others via a consent model with the citizen in control. It allows citizens to track who uses their data, update their data once and then cascade this through public service databases, auto-populate forms from their existing data and, if desired, share this data with third party service providers to enhance their services for the citizen – all without a centralised database.
7) Develop a personally held record

   a) True ownership – where the Exchange Layer allows a view of ‘tethered’ records (i.e. those held in public service databases), ownership and transparency would be further enhanced if an ‘untethered’ record was fully held and controlled by the citizen.

   b) General Data Protection Regulations – the key test of ownership is three-fold – 1) active, not passive, consent to share, 2) the ability to withdraw consent at any time, and 3) the ability to delete your own information entirely. An untethered personal record would satisfy this requirement.

   c) Choice – in Finland, Holland, and increasingly in other identity schemes such as for the UK Government’s Verify, citizens are encouraged to choose a third-party provider to exert their ownership at arm’s length from a central authority. A marketplace should be stimulated for the untethered personal record, in which citizens should be able to use government credits or their own funds to select a provider that aligns with their own needs – be it principles, ethics, data storage location, reuse of data for commercial return, or interface.

   d) Shift the balance of control – over time, as it became clear that a privacy-concerned citizen was generating and holding better quality information on themselves, models of care would evolve to be driven from a personally held (untethered) record managed entirely by consent.

8) Capitalise on the infrastructure – demonstrate the benefits:

   a) Develop systems to support decision making – the advantage of these sorts of open, interoperable systems is the availability of data subject to consent. This will have benefits purely from a citizen empowerment point of view – however the other main benefit will be in the ability to support decisions made by professional and informal carers, ideally with the citizen, about the best course of action for care or treatment.

   b) Develop preventative approaches – powered by this shared data, care models could evolve that consider a more holistic view of the citizen and understand what events and trends may lead up to an issue. For example, deterioration in sleep ahead of an asthma attack, or reduced activity outside of the home as someone becomes more frail. If constructed on the citizen’s terms, this could offer reassurance to them and their families that they would be offered help when it is needed, and in many ways, allow them to retain their independence safe in this knowledge.

9) Secure political will – most of the value described above comes through properly interoperable systems. However, interoperability is not only a technical concern. It has political, legal, organisational and semantic components. In short – this sort of eGovernment will not manifest without high level leadership and willpower to align capability and resources to the opportunity. The resource implications of a shift in service delivery of this kind are significant. However, it must be noted that capability need not only come from public coffers - industry partners are willing to contribute resources to the co-development of these
solutions – and do not need exclusive or privileged access or rights to do so. They are looking to enhance their own understanding of this new marketplace and only require confidence that when they commit resources, there is a reasonable chance of implementation at scale should the solutions prove effective.

10) **Start a national dialogue** – linked to the political will and citizen-centred design points is the need to have a national dialogue around eGovernment. Distrust in government around data sharing comes when it is perceived that the citizen has no control, and when public services are seen to negotiate data access for their purposes, rather than for a citizen’s direct benefit and articulated need. Instead a programme of research and design activity is required to understand acceptability of data sharing in the context of an empowered citizen jointly managing their own care. This can then inform a national dialogue that helps the country consider the options and understand how citizen ownership of their identity and data can drive a more seamless and effective public service offering to meet their needs.

### 4.3. Broader eGovernment Development for Future Care Integration

This section heavily paraphrases the European Science Foundation (Rigby, Keeling, & Hill, 2013).

Most European countries are now trying to integrate health and social care to provide more holistic, citizen-centred, community-based and integrated care. This adds a new dimension to debates about identity, data sharing, privacy and empowerment.

Reflecting on some of the trends highlighted above, they conclude that:

“the vision must move from electronic records for individuals to authorised access to inter-communicating record systems, which together give all the necessary information needed by a specified user for a specified purpose and context at a specified time regarding the individual. The research needed to progress this is not into technology (though developments in systems such as intelligent brokers is important), but into the issues of standardisation, terminologies, person and practitioner identification, indexing and governance, coupled with related studies of usability, intuitiveness, and education and training of users and of data subjects – the people-based issues.”

They call for social - technical research and policy development, with the following key needs:

1) **Citizen Identity** - needs to be consistently established in a trusted way in order for integration of citizen-centred care to be achieved.

2) **Professional Provider Identity** – needs to be consistently established in order to build trust between service providers in the circle of care around the citizen.

3) **Informal Carer Identity and Linkage** – this circle of care is incomplete and usually invalid without the inclusion of informal carers. Citizen-centred care depends on this full circle being created, and in many cases with linked or delegated authority for an informal carer. This is
very difficult to achieve without some sort of citizen identification for both care receiver and informal carer.

4) **Privacy and Data Ownership** – systems need to be developed that protect the professional’s capability to offer effective care, while allowing a citizen the ability to limit the information being shared if desired. Informal carers must be accounted for in these systems.

5) **Autonomy, Access and Ethics** – in the event of a hospital attendance or emergency, citizens are reassured by comprehensive, integrated care records that link up all the people and processes required to ensure they have seamless and effective care. However, as care extends into their home and personal lives, some may be reassured by this integration, while others may find it intrusive. Research and design activity must explore:
   - how to make this integration acceptable and useful for integrating care in the community.
   - development of intuitive, citizen-centred interface, control and choice mechanisms. For example, to govern “agreement of who is in their informal care team, structured levels of information sharing, and client-determined differential access control algorithms, which, in turn, need to be backed up by the development of governance systems and related audit and sanctions.”
   - There must also be mechanisms for dealing with loss of full mental competence, and with conflicts between different involved parties.

**An Enhanced Set of Personal Data Services**

Integrated care will require joint objectives for the virtual care team, determined using plain, common language, and in cooperation with the citizen who will take a central role alongside informal carers as appropriate. There needs to be a clear way of recording these objectives, as well as choices and preferences regarding the methods of achieving them. The roles and responsibilities for the various activities should be captured, and then any unmet skill requirements highlighted. This should then be shareable as appropriate. Key features of these sorts of services include:

- **Citizen-Based Differential Access Control** – “Whatever models are developed, final authorisation for setting access levels must lie with the citizen, who should be able to give protection to specific parts of their record, and to be able to give identified individuals, or functional groups, specific levels of access. For simplicity, this may well be based on a default model, but the options should be easy to apply. Further, means of citizens nominating a named trusted agent to exercise certain functions should be included.” (Rigby, Keeling, & Hill, 2013)

- **Data Contributions** – “Not least for reasons of veracity and trust in accuracy, only professionals and employed carers traditionally have been able to make record entries – though some exceptions such as patient diaries and patient completion of assessment questions, have value in specific settings. With increasing empowerment, and health co-ownership, this is increasingly seen as unnecessarily paternalistic as well as inefficient. There can be value in clients and their informal carers recording feelings, and functional changes, as well as vital sign self-monitoring, so as to inform the overall care process. Development of types of record adjunct, and criteria as to when the data should be included in the formal
record, or the professional carer alerted to changes, need special study.” (Rigby, Keeling, & Hill, 2013)

- **Data Definitions** – “Vocabularies refer to the sets of terms used, and definitions can be attached. Taxonomies set terms into a structured, often hierarchical context of meaning. Ontologies are means of cross-linking different sets of terms. With the development of information science, vocabularies and terminologies are much more studied, but still remain specific to a professional area. Computing power gives opportunity to automate ontologies to cross-link terms, but the context-specific definitions and ground rules must be determined first. If workers from different health and care domains are to communicate safely, and if clients and informal carers are to interact with this, then much work needs to be done in developing these concepts.” (Rigby, Keeling, & Hill, 2013)

An OECD National Science Foundation international workshop (Rigby, 2011) aligns with this, identifying the need for a “Charter of Subject Rights for Electronic Record and Care Delivery Systems Containing Social Care Data”, recognising the rights of the citizen:

- to access not just recorded historic data but also dynamic data such as forward schedules;
- to express and record their own views and preferences;
- to record observations on their own health, functioning, and needs;
- to decide personal directions on individualised rules for information sharing to formal and informal third parties involved in care or family support;
- and to explicitly qualify rights of defined appointed representatives and agents.

5. Implications for Scotland

5.1. **Current Principles and Strategy**

This section analyses some of the publicly available strategy and policy from the Scottish Government in the context of the broader European lessons highlighted in this paper.

5.1.1. **Identity & Data Sharing**

The High Level Operating Framework for Scotland’s Digital Future (Scottish Government, 2015) highlights the following principles. The table below offers a version of these principles that reflects the difference in tone and intent when Scotland is compared with the countries leading on accessibility and usability of digital services.
Scottish Principles | Finnish or Estonian Derived Alternative
---|---
Having a common approach based on Enterprise Architecture concepts and principles in all sectors will create a common framework and language which will assist organisations to communicate more easily when opportunities for re-use, convergence or cross-sector service delivery is required. | All public services will comply with a single, overarching approach to enterprise architecture that supports the e-Society programme. ICT investment project proposals of any scale will be decided upon by one national group.

A cohesive overview of data is required to ensure a consistent approach is taken and common standards for data will need to be considered. All work in this area must comply with the legal framework for data sharing, respect for individuals' rights to privacy and confidentiality and consider public confidence about when and how personal information is shared. | A single exchange / integration layer will be developed that requires the use of common standards. Every public service is legally required to open its databases and registers to this layer. The layer will operate to the principle that citizens only need to enter data once and that it will be reused until they update it. Citizens must be given oversight of how data is shared and used on this layer, and must be able to withdraw consent at any time.

Public services will be integrated into a shared approach to identity and authentication management. | There is a national identity managed by a separate trust centre. National ID use is mandatory for citizens, though there is no legal penalty for not adhering. The scheme allows seamless and effortless access and authentication for public services. This identity allows the exchange layer to draw together relevant data from all public databases and allows the citizen to gain oversight and control of their data. The citizen can then use their own data to power any service they need.

Scotland and Finland / Estonia have taken different approaches to the combination of enterprise architecture, data sharing and identity management.

The Scottish approach to the concept of identity is understandable given the negative media and political pressures exerted the last time this was openly discussed. However, the world has moved on, and in an era of porous and interlinked global databases a citizen’s data is already traded in a variety of ways, by both public and private sectors.

In this context, countries such as Finland and Estonia have developed and mandated a national identity scheme paired with a compulsory public service integration layer. This is an enabler of accountability and transparency in the way the public sector uses data, and has stimulated a culture in which citizens feel a much greater degree of ownership of their own data, can hold government to account on its use, and therefore trust their governments more.

Currently the Scottish citizen is identified and / or authenticated through a range of means including the NHS CHI number, benefits account numbers, council tax reference numbers, the National Entitlement Card, Drivers licences, YoungScot, Mygov.scot MyAccount, etc. Currently citizens have
little to no control over or transparency with respect to most of the data associated with these accounts and cards - many of which are not voluntary. In many cases these organisations have data sharing agreements to link databases to enhance the services provided to the citizen, but this is not seen by the citizen. This all persists because of the lack of will to unify these methods into one identity scheme with citizen ownership of this identification.

As of now, Scottish citizens have little control over their own data, and also do not enjoy the seamless service benefits enjoyed in countries that have national identity schemes. MyAccount is well positioned to become a national identity scheme, but because Scotland has not had a robust national dialogue, there is little ‘ownership’ of the MyAccount identity on the part of citizens. This is a ‘worst of both worlds’ option.

In parallel, Estonian and Finnish citizens enjoy the ‘best of both worlds’ - they can use one method to identify themselves for all services, and have the ability to consent to efforts to join this data up to improve the service they receive (e.g. auto-populating benefits forms, parking permit applications, etc.) They also have access to how services are using their data because any such use has to be associated with their identity and they can withdraw consent at any time, holding public services to account and protecting their privacy to a far greater extent than is possible in the disjointed and voluntary model running in Scotland.

5.1.2. The Personal Health Record

A eHealth position paper discussed in the Scottish Parliament noted:

“The Government has set an objective that by 2020 citizens will be able to use a citizen “portal” to access a personalised view of their health and care information, enhanced and presented as required to make it accessible, informative and useful to them and their carers, and where appropriate make their own contributions to the information, thus sharing it with the relevant health and care professional. They will also be able to access authoritative information about managing their health, prevention and self-management of conditions. In addition, they will use secure two way electronic communication with their health and social care providers to book and manage appointments, order repeat prescriptions and, where appropriate, use eConsultation facilities, resulting in convenience for individuals and reduced transaction and administration costs for health and cares services. A “portal” should not be interpreted as being a website or an App. Instead, it is the mechanism through which information is exchanged using a “platform” that draws information from the appropriate sources and sends it to the appropriate destinations (information stores, computers, tablets, smartphones, clinical instruments, sensors, etc), while applying the necessary privacy and consent controls.” (Scottish Government, 17).

This set of requirements was codified into the ‘National Patient / Citizen Portal’ project. Since this point, various features have been considered and then plans put in place for a phased development.

However, this description above is an amalgamation of many capabilities, and the nuances between these different functions may be lost when this is considered as a ‘portal’ – which, as discussed earlier in this paper, has its own limitations. This next section breaks down the Scottish Government’s
statement above into a list of requirements and sets them in the context of the European experience and emerging understanding of the enhanced access and usability of digital services.

<table>
<thead>
<tr>
<th>Scottish Government Requirement</th>
<th>Capability</th>
</tr>
</thead>
<tbody>
<tr>
<td>A view of their record</td>
<td>This is possible through a traditional Patient Portal with a unique ID reference number linked to several disparate databases.</td>
</tr>
<tr>
<td>Carer access to their record</td>
<td>The ability to identify both the citizen and their carer(s) and delegate authority to them. Achievable within a Patient Portal.</td>
</tr>
<tr>
<td>Personalisation options for their data</td>
<td>This becomes difficult within a centralised, state-controlled system. This function is likely to be superficial within a web based National Patient Portal. This would be easier if the citizen had options for the interface at a local level or through their own preferred app or service interface.</td>
</tr>
<tr>
<td>Make their own contributions to the record</td>
<td>Basic demographic changes – e.g. contact details, next of kin, etc. are easily handled within a Patient Portal. Deeper contributions – e.g. a citizen’s ‘story’, objectives, preferences and plans would be more appropriately stored in an untethered Personal Health Record, kept separate but adjoined via a consent model to the main record. This type of activity is deeply personal, requires a high degree of personalisation and should be held and formatted as local to the care setting as possible, entirely on the citizen’s terms but meeting basic standards to make it actionable by others.</td>
</tr>
<tr>
<td>Sharing their data with professionals</td>
<td>Any data input by a citizen or informal carer that may affect a treatment or care decision needs to be stratified for integrity and risk. Data provenance is crucial. A common domain ontology and set of standards for different data input types needs to be created to help build joint understanding and trust in citizen-generated data. This is beyond the functionality of a Patient Portal, or any centralised system. A distributed, standards based approach is required.</td>
</tr>
<tr>
<td>Access guidance about their health</td>
<td>Possible within a Patient Portal. The Finnish model is developing such guidance to be live and interactive, feeding from both the EHR and (Untethered) PHR to auto-populate self-management tools, personalising even the simple pursuit of guidance effortlessly. However, this requires an Exchange Layer, Identity provision and consent-driven access to both an EHR and PHR.</td>
</tr>
<tr>
<td>Secure, two-way communication with care providers</td>
<td>Possible within a Patient Portal. However, one of the first ‘rules’ of user-centred digital design is “do not create a new, bespoke communication channel”. If the service is personalised, it will be delivered via a medium they are already comfortable with. For many this is something as simple as text messaging. All that is required is a consistent means to assure identity for both participants in the communication.</td>
</tr>
<tr>
<td>Book appointments</td>
<td>Appropriate for a Patient Portal.</td>
</tr>
<tr>
<td>Order repeat prescriptions</td>
<td>Appropriate for a Patient Portal.</td>
</tr>
<tr>
<td>Virtual or e-consultation</td>
<td>Appropriate for a Patient Portal. Some consideration should be given to these virtual consultations being made available within existing consumer offerings e.g. My Diabetes My Way, rather than at a centralised location only.</td>
</tr>
<tr>
<td>--------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Mechanism to draw data from care service databases, citizen-held records and citizen apps and devices</td>
<td>This is traditionally seen to be part of the Patient Portal proposition – at least for the state-held electronic health record. However, due to the extremely diverse set of data sources and user needs associated with this transfer of data, it needs to be decoupled from the Patient Portal ‘single point of access’ interface. Instead the Patient Portal (as an interface) should use a separate, pan-public service ‘Exchange Layer’ to draw data from any relevant source, with rules around certification, consent, security and identity built into the layer. In this way a number of interfaces could offer this functionality, preserving citizen choice and personalisation across many services – health, care and broader public service.</td>
</tr>
<tr>
<td>A consent model to safeguard citizen ownership and privacy</td>
<td>This need to exist beyond the Patient Portal (and indeed the healthcare) use case. Any use of any citizen data should be governed by one, cohesive national consent model, and then deployed on an exchange layer common to all public and citizen held databases. This in turn can also allow the citizen to have a unified view of who is using their data and the ability to withdraw consent effortlessly when appropriate. This can then in turn only be realised with a unified, citizen-owned national identity.</td>
</tr>
</tbody>
</table>

The infrastructure that sits beyond a centralised health interface is recognised in Scotland’s broader strategic approach. Scotland’s Digital Future: Delivery of Public Services Action Plan 2015-2020 (Scottish Government, 2012) outlines a vision in which “citizens readily know how to and can access personal information held about them, allowing them to confirm accuracy and to choose if they wish to create their own personal data store” and “citizens feel confident that personal data is being shared responsibly to create better and more responsive services which meet their individual needs”.

The Health & Social Care Information Sharing Strategic Framework (Scottish Government, 2015) determines that “partnerships should review existing processes to ensure greater involvement of people in creating and contributing to the information that underpins their care and support.” Section Four of this framework outlines actions to deliver on this principle – namely – “Scottish Government to develop plans for a public debate on how people should be enabled to play a greater role in creating and sharing health and care information”. However, the action timescale was left as ‘TBC’ and it would seem this public debate never took place.

The lack of public debate means that more systemic change of the kind found in other European countries cannot happen. The more fundamental digital building blocks highlighted in this paper require a dialogue and proof of the acceptability of the identity and consent-driven sharing of personal data across public services. In lieu of this debate the Patient Portal concept is appealing – it would require change only to NHS-controlled resources such as the EHR, CHI registry and the creation of an NHS login. It would add much needed functionality from a service point of view in the form of appointment and repeat prescription booking in a centralised, cost-effective manner.

However, in pursuit of a national single interface that aspires to load all the previously listed digital health and care functionality behind it, we are in danger of defaulting to a format that centralises first and personalises second, and is based on how the health and care system would like citizens to
behave, rather than being responsive to the reality of how they will behave. This is a format that has been repeated over the years and sees the UK 20th in Europe for usability and accessibility of digital public services.

Rigby et al (2015) summarise the issue well, stating that: “Most current evaluation studies have focussed on the immediate and somewhat mechanistic access to the current record, held electronically, within current philosophies of a professional-client service relationship. Something of a paradigm shift is needed to move to how the new, technology-supported, patient-centric coordinated care is organized with the citizen central and by no means subordinate. Here evaluation needs to be one of communication as an aid to co-production, requiring very different constructs and measures. Then there is the further complication and barrier, that even modern services are too frequently designed by educated professionals and policy makers for ‘People Like Us’, and thus still fail to serve the disadvantaged and societally disconnected, even though they are known to have greater health needs.”

Instead, the broader set of capabilities beyond the traditional portal approach needs to be considered, and must be built upon a dialogue with citizens focused on the desirability and acceptability of modern data sharing to support digital services on their terms.

5.1.3. Case Study – A Personal Data Store for people with Multiple Sclerosis (MS)

One example of this citizen-centric, co-produced approach comes from the DHI’s work with people with MS. The findings were as follows (DHI, 2017):

The concept of a person-owned data store (or ‘Backpack’ as the users called it) that would allow the person to securely manage and share their personal information was positively received by both people living with MS and health and care service providers.

People living with MS highlighted several characteristics that support positive interactions with people and services, which can be translated into design principles for the structure, language, look and feel of the Backpack. Insights about security and data sharing suggest that participants were pragmatic about the risks of loss of privacy in exchange for the perceived benefits of convenience and equitable access to information, empowering them in their interactions with statutory services. Participants highlighted the importance of designing the Backpack to accommodate and reflect their personality and interests, facilitating everyday life and activities. Health and care professionals would also value this information, supporting them to understand what the person enjoys and tailor their care to their aspirations.

Health and care professionals could see how the Backpack would overcome many of their current challenges in: accessing information from other health and care professionals, better understanding the needs and wishes of their service users and managing increasingly large case-loads.

The four design concepts presented offer insight into how people living with MS and health and social care professionals would envisage person-owned data stores working for them in practice, offering a fresh perspective to existing conversations between technologists and Government strategists. These concepts include:
1) **Mapping Interactions** – making visible the complex interactions of multiple carers with the citizen.

2) **Health Story** – offering a way for a person to tell their own story their own way, to do this once only and then use this and their preferences to drive the way they want their care delivered.

3) **Smart Form Filling** – allowing benefits forms to be auto-filled from the Backpack, significantly reducing the emotional burden this process places upon the person.

4) **Tools for the MS Specialist Nurse** – this is a staff facing view of the backpack, that allows the specialist case worker a dashboard view updated whenever the person or another care professional changes or updates information in the Backpack that might mean more or different support is needed.

The benefits of involving citizens and health and care professionals in this conversation are highlighted by the innovative and practical nature of the proposed concepts. Their ongoing participation is vital to ensure that any developments in this area meet the needs and aspirations of the people who will use them.

### 5.2. Recommendations for Strategy Going Forward

In summary, to close the gap between Scotland’s high level of overall digital progress and relatively low levels of access to digital public services the following recommendations are made:

1) **Renew some basic principles** - better recognising that:

   - **There is a balance of benefits** - between consistent, centralised digital infrastructure and more local and diverse use cases and interface needs.
   - **Personalisation** - can be the customisation of a generic ‘whole system’ service, but it is more effective to design a range of interoperable services that are built from first principles to meet end user needs.
   - **Access to data is not ownership of data** – and that empowerment is limited when ownership is limited. The concept of an untethered Personal Data Store (so beyond just a health record) must be pursued as a means integrating new service models, driven by the citizen.
   - **Meaningful contribution to co-management of care** - means the joining of two equally important sources of information, preferences and plans (the care provider and the care receiver), not just the ability for citizens to customise or feedback on services as they are.

2) **Learn from international experience** - there are common features adopted by the European countries leading on both the development of digital public services. These could be pursued to support upcoming strategy work:

   - **Think beyond health and care** – much of the value will come from non-health and care sources.
   - **Distribute services** – centralise only standards and common, open, enabling infrastructures.
• **Partner with, don’t just procure from, industry** – who can flex and personalise a citizen’s digital interfaces and tools, while generating economic value for Scotland.

• **Centre design on the citizen** - drive the development process by understanding how citizens want to engage with digital public services – do not digitise current processes.

• **Develop a common approach to identity** - that enhances ownership and transparency around personal data and enable new personalised digital services driven by consent.

• **Develop a data exchange layer** – that supports the consent-driven reuse of data through an open, secure and standards-based intermediary layer that all public service databases can connect to.

• **Develop an ‘untethered’ personally held data approach** – that offers true ownership of personal data and the means to securely consent to the sharing of this data to power services that meet citizens’ needs in a flexible way.

• **Capitalise on the infrastructure** - for enhanced, joint decision making and preventative approaches to care.

• **Capitalise on the infrastructure** – for integrated care – enabling consent-driven data sharing between partners and allowing a citizen to drive care planning from their own personal record.

• **Secure political will** – this approach to digital services has political, legal, organisational and semantic components – not just technical ones. In short, this sort of eGovernment will not manifest without high level leadership and willpower to align people and resources to the opportunity. The resource and capability burden can be shared with industry to reduce the public sector costs while stimulating the local economy.

• **Start a national dialogue** – linked to the political will and citizen-centred design points is the need to have a national dialogue around eGovernment. Distrust in government around data sharing comes when it is perceived that the citizen has no control, and when public services are seen to negotiate data access for their purposes, rather than for a citizen’s direct benefit and articulated need. Instead a programme of research and design activity is required to understand acceptability of data sharing in the context of an empowered citizen jointly managing their own care. This can then inform a national dialogue that helps the country consider the options and understand how citizen ownership of their identity and data can drive a more seamless and effective public service offering to meet their needs.

3) Re-profile the Patient Portal activities

We should renew our understanding of the different components required to achieve the 2020 commitment. Breaking these down into two development tracks:

1) The Patient Portal should proceed based on reusing existing capability rather than creating something bespoke. It should focus on the transactional benefits commonly associated with Patient Portal technologies in the short term to yield benefits primarily for health and care service delivery. Activities would ensure that a citizen could:
   • Access their Electronic Health Record or let an informal carer do so,
   • Edit basic demographic information – potentially linked to the CHI registry,
   • Access static guidance about their health and care,
   • Book appointments and repeat prescriptions,
• Securely communicate with professionals via messaging and virtual consultation.

2) Initiate and resource innovation activity to explore how the citizen wants to engage with digital public services and then develop appropriate, interoperable solutions to support this in a manner that is congruent with the Patient Portal development. This may yield several digital infrastructures that are more fundamental than the Patient Portal, and that might span more than just health and care needs. Activities would ensure that a citizen could:
• Personalise their own record and information,
• Make contributions around their life story, objectives, preferences, and care planning,
• Share data they generate with professionals,
• Take advantage of an exchange layer that joins up data to offer personalised services,
• Connect consumer devices into their records in the context of novel self-management services,
• Develop a high degree of control over their own data, with consent driving data sharing.

5.3. Conclusion

This paper has planted some flags for developments Scotland is primed to undertake. We have the capability and technology already, and while other countries have been first to demonstrate the potential, Scotland has a better starting position than many of our European peers due to our cohesive policy and strategic approach driving towards citizen-centred, integrated care.

Realistic Medicine, as espoused by the Chief Medical Officer, can be achieved by enhancing our ability to share data in a consent driven fashion, allowing more seamless and personalised services, with diversity for citizen but built on a consistent core infrastructure and standards base. Key to this are three interlinked concepts:

1) If the citizen is to be empowered, then they must own their own data, must see the data held by other about them and must be able to limit how data is shared effortlessly and directly
2) Care is distributed – so the digital infrastructure must not centralise power and access.
3) Personalisation is more than just customisation of generic services - permission-less innovation must flourish near the citizen, but within a governed set of standards and norms to protect quality of care.

A distributed care system supported by a distributed, but standards based digital infrastructure, is exactly what the Scottish digital health and care marketplace needs to flourish. The leading e-societies of Europe are now capitalising economically on their open, distributed, data rich systems. Businesses are able to add value significantly quicker with far fewer barriers, and can demonstrate benefits directly to citizens. This in turn then allows them to engage with global markets that are increasingly working to the same consumer focused, distributed delivery models.

One remaining barrier to progress in this area is the issue of privacy – especially as this links to the politically sensitive nature of a unified digital identity. However, there is no need for a mandatory
identity scheme now – many of the benefits could be achieved within the health and care domain by the relatively simple development of an untethered personal data store that can be linked to the CHI number and / or MyAccount with the citizen’s active consent. Those groups that need integrated care and ownership of their own data could achieve this in the immediate future, and this in turn could help Scotland understand the benefits of this type of citizen empowerment.

6. References


