medConfidential: Available next steps in Patient Online (March 2017)

The Department of Health has political priorities which do not necessarily include upgrades of underlying technical infrastructures. Parts of “Patient Online” date back to 2013 and earlier - they predate NHS England, and have been upgraded and repurposed for additional priorities.

As NHS Digital looks towards an NHS-wide login infrastructure, presumably one based on replicating the Verify hub and privacy model, there are a number of client-based upgrades that should be considered critical and which resolve outstanding questions.

It is worth remembering that the current access method was developed a number of years ago, where the problems of implementing a novel digital service were different to those that must be considered by a mature service.

It is a design principle of this document that nothing requires any change in activity by any GP compared to what they (are contracted to) do now. Indeed, throughout, we assume that credential issuance must be grounded in a pre-existing clinical relationship, which for Patient Online, is and remains true; this is not true of other potential models, such as a taxpayer credential. If the grounding of identity in a clinical relationship is to be abandoned, then there will be workload implications for GPs that are going to be significant and unpredictable, being highly dependent on the digital savviness of each GP’s patient list.

Part A: Patient-visible next steps:

1. Choose and Book should be the first exemplar service

Run by NHS Digital, Choose and Book has both the need and ability to deliver large-scale financial savings quickly, as a digital service that is relatively new and has a clear patient benefit. Given the simplicity of institutional arrangements, this should be done first to gain experience.

The financial benefits of a functional digital Choose and Book service for appointment rescheduling cannot be understated, and dwarf the costs of any other aspects of this work.

Some GPs already offer “same day” appointments earlier online than they do on the phone service (appointments are released at midnight - “same day” - which is earlier than when the phone service turns on). This should aid take-up of digital amongst the most heavy users of services, and also help reduce missed appointments by that category of patient.

2. Patients should be able to enable two-factor authentication for their own accounts

Patients should be able to enable two-factor authentication on their account, in a way which works for them and the devices they have. Two-factor authentication is a fundamental requirement in 2017 for any system that wishes to handle sensitive data.

The GPSoC providers have different apps for smartphones, and two-factor authentication can be added as a feature to those apps using their ability to offer features to their customers. For patients without a smartphone, two-factor (2FA) using either text or phone are both an option.

In due course, 2FA should be mandated. For logins to external services, the digital service assessment should assess whether 2FA should be recommended or mandatory for that service. We expect it would be recommended for most services, and mandatory for some.

Enabling of 2FA in the first instance should be determined by patient choice, as provided by the GPSoC providers through their existing tools, although some education of users is necessary to avoid a "John Podesta problem".[1] Impediments to mandation of 2FA should be examined and removed over time. Two-factor authentication, however, should be a patient choice based on the tools they have already chosen to use, and other work. With DH's focus on apps, that GPSoC providers add 2FA into their apps to protect their app users (i.e. their customers' patients) is not a contractual concern, it is simply an example of medical ethics being applied by technology professionals in a digital NHS.

Such tools would also allow, for example, exposure of audit trails through secured processes where other capabilities have been made available, subject to suitable protections.

Should passwords get stolen, the Patient Online login system should include an additional factor: needing to know for which GP a stolen username/password is valid.[2] It is likely that these are rarely stored (other than by the GPs themselves) which gives the NHS a regulatory assist unavailable elsewhere. Advice should be given on where, other than the GPSoC systems, usernames in bulk may be stored, and the possibility of removing any such risks. The reuse of the Verify infrastructure will help significantly here.

Due to the variety of conditions which NHS users may have, and the threat models they face, there is likely to be a rich vein of opportunity for generalisable user research into novel 2FA methods, e.g. inverse geofencing.

[1] http://www.politico.com/story/2016/10/john-podesta-cybersecurity-hacked-emails-230122

[2] Current practice varies by GPSoC provider. Where there is an existing login page which covers all a provider's GPs, the GP field could be added, or normal routing could change to take patients to a page where that is correctly pre-filled and hidden, e.g. https://nhsverify.medconfidential.org/nhsverify.html. It may also be that there are normal routes which protect this, and legacy routes which do not, and it evolves over time - 'available next steps' focus on a goal, not how to get there, or where people start from.

3. Patient Reported Outcome Measures for 100% of patients with chosen conditions?

In a digital NHS, it is entirely practical for 100% of patients in particular classes of treatment to be offered the opportunity to fill in a PROMS survey for their conditions - including co-morbidities - and to do so at times and with details of their choosing. In effect, these are patient outcome surveys linked to a clinical diagnosis and outcomes within the various Registries.

The first example should be for cancer pathways; with a mental health condition PROM as a fast follower. The principle should be that all pathways should be covered in the medium term.

What would a 'digital first' PROM look like for each patient grouping? With a patient-driven interactive online survey (which is what a 100% PROM would be; "surveymonkey for the NHS") what opportunities for small samples and subgroups can be used with ultra-low-cost ongoing engagement from past patients?

B: Infrastructure

4. Service specific pseudonyms

Following the PCAG principles,[3] each digital service should receive a unique patient service-specific pseudonym to avoid data linkage, alongside the CCG in which the patient is resident. No other information is automatically provided; although for providers who have met all other standards for the use of the NHS number, they may request for it to link internally to existing records, with full audit applied. There should be no other changes to the rules of NHS number handling.

5. No back door lists of service uses

There must not be a 'back door' list of users of particular services within any central authority.

If necessary, as a privacy protecting measure, when a (sensitive) new service is introduced, pseudonyms should be pre-generated for all NHS numbers. Other approaches are available.

[3] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/361496/PCAG_IDA_Principles_3.1__4_.pdf

6. Include the CCG as an asserted attribute

To avoid making worse the long-term problem of identifiable data being used for billing purposes, a CCG identifier should be available as an assertable attribute, and NHS Digital should be in a position to provide assurance (via statistics) that CCGs were only charged for the number of service user patients for whom they are responsible.

Given the administrative complexities of invoicing in the NHS, this problem should not be ignored.

7. Data Incident Protocol

When developing the service standards for access to the infrastructure, a Data Incident Protocol should be developed which ensures that data (mis)handling incidents are properly handled and communicated to patients, rather than being covered up by service providers. Public sector bodies in the NHS are required to report losses to the ICO; others who wish to interface with the NHS should report losses to patients following an agreed protocol.

The ongoing work to tell patients how data is used will make this significantly easier.

C: Digital more widely

8. Cloud hosting standards

Standards for hosting services in the cloud, but on UK soil, should be considered. GDS (and sister services internationally) have done some of this work for their own areas, and NHSD should do the same for NHS services.

9. Identity in the rest of Government

The NHS is not facebook. It does not seek to enforce a “real names” policy, and would cause harm to vulnerable patients by doing so.

While we strongly believe that a clinical identity solution must be grounded in a clinical relationship, we are aware that there is a forceful argument from Cabinet Office that identity provision based on data matching should also be an option for citizens (note, the designation) in principle. While no worked example has been provided, and the operational flaws in this could be catastrophic, if Government wishes to insist on this model, any Central Government identity service should be equally considered. The culture of identity exceptionalism in each Whitehall Department is not likely to interact well with providing direct care to patients via a digital means.

If the intent is to follow treat the NHS as any other Government department and do data linkage via matching, that suggests a dramatic u-turn in policy as DH will have abandoned the multi-decade push to have the NHS number used as a single identifier for direct care, and done so less than a year after the Lefroy Act came into force. That seems like a spectacular waste of time and resources, especially given the reasons that the NHS Number exists in the first place, to solve problems that data matching can not address. With DWP, a matching failure is a bureaucratic annoyance; with NHS data, it can be far more significant.

D: A vision beyond these steps?

10. SH24 at scale?

What else is necessary for novel, digital only, approaches to effective services at scale? What can exist as a solution in the mental health community that uses digital only tools? What is a talking therapy in a digital first world?

11. What does good look like? How can commissioners know?

It is unclear what a "good" digital service for the NHS looks like. What are the .Everyone tests for a good digital service in 2018? *What does good look like? How can commissioners know that?*

What are the tests that commissioners should apply to commissioning of digital services? How will they know good from bad in digital terms as well as clinical terms? Does this reward those who care about user experience, and deprioritise tools from those who don't care? It is all too easy for providers to to deliver for those you're talking to, and harm those you're trying to help. How do you create a race to the top in terms of patient experience for digital services into the longer term? What is the objective metric that will measure this, both competitively and against contemporary standards?

Who will ensure that there are non-exclusionary standards for good and better into the future of a digital NHS, that help everyone? How can they evolve over time?

12. Helping the furthest first?

For those in the care of the state, what opportunities does the only private space they may have for years - their Doctor's consulting room - offer in a digital world to enhance their lives under their own control?

More broadly, throughout digital systems architecture, design and development, the focus should be on individuals as people, considering their experiences and contexts across their lives, not just the time they are in NHS or social care. People in the greatest need will have multiple points of contact within health and social care, are using such services the most, and may be subject to different risks which need specific consideration. Individual services should respect this complexity, and the coordination burden placed on people and the formal and informal care and support teams around them.

medConfidential
March 2017