Getting to safe settings from the status quo

We recognise that the introduction of safe settings into the Health and Social Care system for all individual level data will require substantial systematic change. These changes will be no less substantial than the institutional reform of HSCIC following the Partridge Review looking into treatment of HES and other individual level data sets.

It is understandable that a review designed in around March does not take account of changes in Governance and processes from April - June. However, that does not mean the outcome of the consultation can no take account of exactly that.

Safe settings

HSCIC has stated that care.data records will only be available in a safe setting, what medConfidential has proposed as a Health Research Remote Data Laboratory, following the models of other similar facilities around the UK Government and around the world.

While the Accredited Safe Haven proposal in this consultation is superficially similar where there is any detail, in most areas, it lacks the governance, and independent process features required to make a safe setting actually safe and transparent for individuals who have consented (or simply not withdrawn consent) to their data being in that setting

Using larger compute facilities (primarily at HSCIC), via secured connections running over N3, a safe setting can offer better facilities to a user than they have locally, at a higher level of data safety. An individual can manipulate data they have remote access to, but can not extract data without going through a clear, auditable, defined process.

All data going into the system must flow through a similar (possibly automated) process. With audit possible of the uses of tools inside, and knowledge of what data entered and left, it is possible to have confidence in the system. A demonstration that someone will not “seek to identify” is meaningless, an assurance from individuals and organisations, paired with verification of actions, provides knowledge to patients.

This is a fundamental failing of the consultation; it has underlying assumptions of trust in the decisions of bodies that have been discredited since the consultation was drafted.

It is no longer sufficient for an NHS organisation to trust that data has been handled safely, it must demonstrate that in a way which patients know where their data has gone, and why.

Working Practices

Without clarity on governance and structures, and separation of responsibilities, and an understanding of the data products needed by each function, working practices are difficult to define. It is feasible for working practices to incorporate remote access to a virtual safe setting for defined purposes. As our risk stratification response discusses, deconflating of purposes and the various different stages within purposes allows for comparatively easy solutions, and custom data products.

While we nominally discuss multiple safe-settings, these may be only logically separated with technical measures for enforcement rather than physically or otherwise (so an individual with access to one set of data may not simultaneously access a different application and a different set of data). Again, the remote compute facility has benefits here, due to the data being in one single place, rather than multiple. Audit becomes simpler.

Guidance for safe settings exists for other facilities, including with differing levels of access. Some form of separate, secure, room for individual data utilising a secure remote link to the server, whereas and a remote access facility for lower sensitive data may be accessible from a desktop via overlaid secure connection. The academic Secure Data Service follows this model successfully.

Defining data and purposes

For care.data, the conflation of “secondary uses” caused public concern about one to spread to all. This will be exacerbated if it is not completely transparent, to each patient, about what their medical record has been used for, and by whom.

Any secrecy, any lack of transparency here, poisons the whole system. The majority of decisions may be as transparent as pure water, but it only takes hint of a secret teaspoon of sewage within, for opinions of the system to shift dramatically.

If an organisation has a local copy of data, they will be required to handle fair processing and Subject Access Requests and ensure that only authorised queries are run, which seems an unnecessary process when there is a safer and no less functional alternate. Registers and logs are necessary, but they are not sufficient. This strongly suggests it should solely be an HSCIC host for the data, with other organisations remotely connecting to do their work. HSCIC is now constituting has processes to ensure that audit and tracking is possible. We would have grave concerns about NHS England attempting to replicate this process, without an equivalent to the Partridge review of governance and decision making.

Related to this, every organisation involved must be subject to a meaningful single strike penalty where appropriate. As with the research single strike, penalties must not have a perverse incentive. Organisations which self-report and take steps to rectify should be treated accordingly.

What data?

There is much made of a “digital NHS”. What that means, is a different matter. Past programmes have attempted to be the 1990-style argos catalogue, all possible items, in a 2014 Amazon-prime world of the needed items delivered next day. That big book of everything model, the style of care.data, is can no longer be considered a safe or transparent option.

Sending copies of datasets around was once the only way to use data effectively. It was 2007 when HMRC learnt the downsides of that approach. Posting the medical records to external parties, granting them the capability for unconstrained discovery is no longer necessary for many applications. Where individual level records is justifiable, principally in research, the use of a safe setting environment exclusively has already been accepted, whether HSCIC's environment , or an equivalent such as at the Farr Institutes.

There is no reason that every data flow in the NHS should not be the appropriate balance of safe, consensual and transparent. All individual data flows should be able to be audited and logged, to the level that a patient can be told which organisations have access to their records. The advantage of creating clear data definitions for purposes, is that the process scales and can scale. It needs to.

The consultation is unclear what data is actually being proposed for use. It must not be arbitrary individual level data for arbitrary or vague purposes. That is the approach that failed multiple times with care.data in 2013 and early 2014. The lessons from care.data must be learnt, and the lack of clarity here may have negative consequences if the public is surprised.

Following the model of QOF

The QOF dataset is incredibly complex in design, but relatively simple in output. It takes detailed and intricate queries, and produces a set of aggregated counts as output. What has been done for QOF can be done for each other relevant purpose, with generally lower complexity and greater transparency. Every data flow can be justified, with what data goes where, and why, being recorded. As the NHS evolves, and changes, these can also evolve simply and easily alongside, as each flow is small and simple.

The alternative, the model care.data attempted, is to create an opaque big pot in which all data gets poured in, and arbitrary data extracted, and any sewage in the pot immediately pollutes the reputation all data flows. The QOF model shows that doesn’t have to happen.

Every data flow in the NHS can be the appropriate balance of safe, consensual and transparent. That will not only build trust in NHS data handling, but it will do that by building knowledge of NHS data handling of each patient. Blind trust will be unnecessary, as these will be defined flows that can be known.

There is no reason that NHS data flows should rely solely on public trust, they can be based on public knowledge if the systems chose to inform the public.

Sam Smith
MedConfidential
August 2014