

## **medConfidential submission - a longer term NHS view**

As the NHS begins its cycle of some longer term thinking, there are a number of principles that can be embedded now, to avoid repeats of past problems. Over the course of the period covered, there will be NHS legislation; many of the problems that the NHS and DH have struggled to address in two years can much more easily be solved within ten.

Within the scope of the Long Term Plan, possibly in the legislation that may follow the ACO consultation, **the National Data Opt-Out should be placed on a statutory footing**. The non-statutory implementation should be complete by March 2020, and a statutory basis should raise the confidence of patients. While this may not be an urgent commitment, it should be a definite commitment.

Every data flow in and around the NHS should be consensual, safe, and transparent. Patients should be able to see how their data is used. Many of the innovations envisaged in and for the NHS will require patients' data. If the NHS wishes to use data in 'innovative' or potentially risky or controversial ways, the trust that is built from transparency of projects and governance will assist in the successful delivery of such projects. Lack of it will not.

NHS Digital's commitment to a 'remote data environment' should be expanded to maximise the safety of data handling throughout the NHS. Otherwise, every data project will be weighted down by the failures of care.data, and the institutional failure of NHS England to believe it has any lessons to learn from that failed programme. Currently, the most straightforward way for a patient to see how their data has been used is at [TheySoldItAnyway.com](http://TheySoldItAnyway.com). The Citizen Identity project, due to launch shortly after this consultation closes, should make showing patients how their data is used entirely feasible.

**All patient-level data should be treated as identifiable**, unless a dataset is specifically created to satisfy an obligation in line with the UK Anonymisation Network framework on Anonymisation (which is already updated for GDPR), and the forthcoming 2019/20 GDPR update to the ICO Anonymisation Code. While it may make NHS Digital's work easier to have a few datasets used for many purposes, this increases the risk for patients – and other NHS bodies, which have more data than they truly require (in itself a failure to follow the 'minimisation' principle of data protection law).

All the information governance protections – including promised safeguards and sanctions – that patients are told will protect them, must be functional and resilient. This is still not the case, even in current communications.

There are many reasons for the NHS to use patients' data and, in the longer term, it should not be afraid of making the case for each of these uses to patients. In any event, it will have to. The question is whether it does so strategically and with confidence and clarity, or only in response to cockup or catastrophe.

## CCGs/LHCRs/STPs/ACOs/ICPs/etc.<sup>1</sup>

Direct care, and management of the NHS, both require a reliable data infrastructure that satisfies necessary data protection law, the common law duty of confidence, and other obligations on which the NHS as a whole and in each part must deliver.

*For direct care*, creating data silos by regions/CCGs/STPs, etc. will eternally lead to problems where those 'inconvenient' patients cross an arbitrary administrative boundary, created by the NHS. Data silos should be avoided, and interoperable systems used to ensure that a clinician with a direct care need can access relevant, timely information.<sup>2</sup> To deliver on such a requirement, patients must have confidence that they can see who has accessed what information when, to know that their data has not been accessed inappropriately. Where a record such as the SCR should have been accessed for direct care purposes, but was not, showing a patient where their record was *not* accessed could offer powerful evidence to increase the take-up and usage of such systems to aid patient care across the NHS estate.

*For secondary uses*, over the course of the time periods being considered, NHS England, CSUs, whatever CCGs turn into, and other levels of the NHS will have to resolve the many data issues ignored since NHS England was founded. A top-down commitment to full transparency and a coherent data infrastructure will allow an informed discussion about how data is used, and how data should be used. The National Data Opt-out must clearly apply across the entire system, and all secondary uses of NHS data should also be in a register – in addition to being able to be seen by patients whose data was used.

Many of the complex questions facing data-using services will be significantly simpler if, over the long time periods being discussed, NHS bodies have a mechanism to routinely and centrally provide information so that patients can reasonably expect that, should they wish to look, they know how their data is used.

medConfidential

September 2018

coordinator@medConfidential.org

---

<sup>1</sup> This is not an exhaustive list of relevant acronyms, but we trust you get the point.

<sup>2</sup> <https://medconfidential.org/2018/local-health-and-care-records-exemplary-or-just-more-of-the-same-old/>