

Dear NHS England,

Implementing NHS secure data environments to enable research and development

I am writing to you in my capacity as a Public Advisor with the NIHR Applied Research Collaboration North West Coast (ARC NWC), and as a Co-Lead of its Care and Health Informatics (CHI) theme. I have some observations to make on the implementation of the recently awarded *Wave One Secure Data Environment (SDE)* initiative for the North West.

Working with the group of quality researchers in CHI, my least rewarding experience has been listening to endless stories of frustration and delay as they try to access the data needed to do important work of benefit to patients and the public. What research gets done and with what timeliness seems, to be far too much determined by what data can be accessed – than by its importance for better health outcomes. This cannot be right and any move to address the situation has to be a top priority.

Clearly, this is much more than a simple question of easing access. The data in question are for the most part private and personal - gathered against a strict code of ethics that safeguards the population in their interaction with their doctors and other medical professionals. This is vital and entirely proper. The difficulty is that we need good data for research but we also need strong data protection. The SDE approach is a worthy and creative solution under development that seeks creatively to resolve this paradox.

Trust with pragmatism is the key that can open the door. The benefits from ready access to health data collected to clear technical standards and assembled at scale are demonstrably enormous, and the NHS probably has the best prospects in the world for the assembly of big data in this domain. There should be no difficulty at all in supporting the regional SDE idea on these grounds as an entirely appropriate mechanism for moving forward. There are, however, concerns about which assurance is needed.

The digital transformation has provided a fast-developing platform for the collection of big data on health on an unprecedented scale. This brings to bear another critical dimension for trust and security to patients and the population in respect of their personal data. The health data they would be invited to surrender under a trust-based covenant (like the five “safes”) to be lodged within an SDE can potentially have both public *and private for profit* value. Maintaining trust even locally, introduces the need for “higher-level” safeguards. These would be *internal to an SDE* and bear on beneficial ownership of any assembled data it might contain for the long run.

Sensitive data residing within an SDE (national or regional) would require (legally enforceable) long run assurances that it would be dedicated exclusively to *public benefit*. We live in a world where a handful of dominant corporate hyper-corporations have a unique capacity to control the big data technical domain and where examples already exist of UK health management systems being sold internationally.

There is then a need to move on from the realm of “principles for trustworthiness” - where excellent work has already been done on “safes” and standards - to the consideration of *confidence-assuring governance structures* for SDEs. Patients and the public need to have confidence that, even though we are talking about something as dry as data, there are systems in place to ensure that the agreed principles of ethics and integrity for SDEs are maintained.

Garnering support for data access would be facilitated by engaging patients and the public formally in SDE local governance and, perhaps more importantly, a campaign should be mounted to persuade people of the *huge public benefits that can arise* from better access to their personal data – working simultaneously then on *trust and pragmatism*.

Peter E Lloyd

Professor (Retired) and Public Advisor ARC NWC; Website: <https://peter-lloyd.co.uk/>