**Opaque and questionable use of patient data by one local Integrated Care System**

A report by *North East London Save Our NHS*  (January 2024)

**Background**

Our personal health data is core to the work of the NHS’s Integrated Care Systems (ICSs), informing not just decisions about our care but also about the commissioning, planning and ‘rationalisation’ of healthcare services. In addition, NHS organisations are coming under growing pressure from the government to share the data they hold on us for research (both academic and commercial), at the same time as legal protections for confidential information are being weakened. It has never been more important to know what ICSs are doing with our data in order to challenge any abuses and poor governance.

With this in mind, we submitted a series of Freedom of Information (FOI) questions[[1]](#footnote-2) to the Board of NHS North East London, the local Integrated Care System We asked about the ICS’s Digital Strategy, its use of patients’ health data (particularly for Population Health Management and risk stratification) and data governance. We also questioned the legal bases that the ICS claimed for its use of patients’ data. (A full report of our findings can be found in the KONP Resources Cabinet – see ‘Health Data).

One of the most disquieting findings was the embeddedness of privately provided data storage and processing services across the ICS. For instance, three companies were named as an integral part of the roadmap set out in the ICB’s Digital Strategy for 2023/4 and 2024/5.[[2]](#footnote-3) We suspect the companies that we came across are just the tip of the iceberg. We also caught a glimpse of the huge costs of data services: for example, access to one of the commercially provided data clouds was available on a ‘pay as you go’ basis, with the ICB charged per-second. We have not submitted FOIs about the full extent of these services or costs as yet, so do not report more on this here.

In this report we focus on just three of the issues that emerged:

1. lack of transparency concerning the governance of data use
2. ambiguity about the use of personal data, especially for risk stratification
3. complacency about how, or whether, patients are informed about the use of their data.

**a) Transparency and governance of data use**

Given that it is central to the functioning of the ICB, there was surprisingly scant mention of data in its publicly available governance documents. An Information Governance Framework stated that the secondary use of patient data was essential for purposes beyond direct care and referred to the work of an Information Governance Steering Group and a Data Access Group. However, neither of these bodies were mentioned in the ICB’s Governance Handbook. At the time of our enquiries, papers from these bodies were not publicly available, and their members did not include lay representatives. However, the Data Access Group, which oversees the lawful sharing of personal data, included two ‘independent’ members, both from private companies. An overview of the ICS’s digital maturity noted that its progress was in line with the national average, but a key issue has been the lack of a digital lead on the main Board and, as we found, the lack of a clear governance structure during the formation of the ICS.

**b) The use of personal health data**

The statutory duties of ICBs (such as a duty to exercise their functions effectively, efficiently and economically) allow ICBs to process health data for a range of purposes, provided that they identify one or more lawful bases to do so. As with other ICBs we have looked at, NEL ICB relies on the UK General Data Protection Regulation (GDPR), namely

* GDPR Article 6(1)(e) – i.e processing is necessary for the performance of a task carried out in the exercise of official authority vested in the controller, and
* GDPR Article 9(2)(h) -.i.e. processing is necessary for the purposes of the provision of health or social care or treatment or the management of health or social care systems and services.

Both Articles allow broad interpretation.

In addition, the Common Law Duty of Confidentiality requires that when an individual provides confidential information expecting that it it will be treated in confidence (as in a clinical context) the information cannot normally be disclosed without that person’s consent. There are though exceptions to this, such as when confidential patient information can be used for the benefit of research or similar activities, in which case an alternative legal basis, such as Section 251 support,[[3]](#footnote-4) must be established.

 That said, the National Data Guardian and UK Caldicott Guardian Chair of Council (NDG & CCC) have expressed concern that, within some data sharing programmes, organisations process confidential patient information for purposes other than direct care without ensuring that their activities do not breach patients’ confidentiality.[[4]](#footnote-5) This concern is particularly relevant to the legality of the preliminary combining and processing of GP data with other data sets for risk stratification (RS) purposes, widely used in Population Health Management (PHM).[[5]](#footnote-6)

Risk Stratification (RS) is used in two ways:

1. to identify patients (e.g. those on a GP list) who are at risk of deteriorating health and may benefit from some form of intervention. Legally, as the processing of confidential data is for direct care purposes, RS can rely on patients’ implied consent.
2. to identify patterns of ill health and health needs across the local population in order, e.g., to plan services. This type of processing is not for individual direct care purposes and so, legally, cannot rely on implied consent.

One of the NDG and CCC’s concerns is that some organisations rely on the concept of implied consent to carry out RS when this is for broader purposes than individual patient care. A further concern is that not enough is being done to ensure that people are aware of how their data is being used.

The NEL ICB’s website provides a privacy notice about risk stratification, which it also calls ‘case finding’ (confusingly it also suggests that RS is a *prelude* to case finding). It further claims that it has Section 251 support to use pseudonymised patient data without patients’ explicit consent in order to plan the most appropriate services for its population.[[6]](#footnote-7)

Approval for this second type of RS is conditional on the ICB issuing a Risk Stratification Assurance Statement and providing a link to their register of the organisations approved to receive and process data for RS. However, when we requested a copy of these documents we were told that the ICB did not carry out risk stratification, only case finding, and only used in-house staff for data processing. Further, in a different FOI response, they said that London ICSs *as a group* were not using organisations to do risk stratification that were not on the list approved to receive and process confidential patient information – implying that RS *was* being undertaken by London ICSs, perhaps including NEL.

It seems unclear whether the ICB is, or is not, carrying out RS; has moved to a different model that can achieve the same aims (with less bureaucracy); or is simply calling RS by another name. This makes it hard to know if the ICB is adequately protecting the confidentiality of patients’ data. What is clear is that, if it is carrying out RS, or otherwise combining and processing patients’ data for non-direct care purposes, the ICB is not ensuring that the public understand the use of their data.

**c) Are patients fully informed about the use of their data?**

We asked what measures were in place to ensure that the public could have confidence in the way their personal information was being used by the ICB (such as for RS). The response was that, as established by the UK GDPR, data controller responsibilities[[7]](#footnote-8) always rest with the individual organisations within the ICS (i.e. care providers such as GP practices or hospital Trusts) that generate the data. The ICB said it could not overrule this. However, while this is true at one level, it seems that the ICB takes a surprisingly laissez faire approach: *it is dependent on the data generated by the organisations within it but takes no part in ensuring the integrity of these organisations’ data collection processes and thus the integrity of the data it uses.*

Similarly, when we asked about the arrangements in place to ensure that the public understands the proposed use of their data for purposes beyond their direct care, the response was that “We have fair processing and privacy notices to document and inform on all uses of patient data”. However when asked at what point in their care journey could patients have sight of such notices, or what was done to ensure that patients could see these notices before their data was collected, the only answer was that “Patients can access privacy notices at any point of their journey”.

Asked where these privacy notices could be found, we were referred to the websites of the ICB and ICS, which would give details of the care providers across the ICS who generated the data and were responsible for issuing privacy notices. *Expecting patients to scour the ICS website for providers and then the websites of those providers to find a privacy notice that patients probably do not know exists, and to do so before their data is collected, is hardly an inclusive way of informing patients about the use of their data.*

Questioned whether the ICB issued guidance to care providers to ensure that patients/citizens have been involved in drawing up fair processing/privacy notices and that these notices are comprehensible to the public, the response again was that “each care provider is responsible for its own data management”. It seems surprising that an ‘integrated’ system cannot establish comprehensive, patient-centred guidance to ensure that the data generated across the system, and that the ICB relies on, has been collected appropriately, including with the full knowledge of patients.

**Conclusion**

Legislation already provides the ICB with huge scope for accessing and processing personal data, while forthcoming legislation is only likely to weaken existing data protections. This ICB’s infrastructure for data use is still in flux and its approach to data processing is opaque, to say the least. FOI requests to other ICBs suggest that NEL are not alone in taking this approach. We suggest that the most effective way of countering inappropriate access to our data is to monitor what is happening at ICB level; demand lay representation on appropriate bodies; insist on the protections that we still have; and demand accountability and transparency on the part of those using our data.

1. Our questions were initially based on those developed during research by the KONP Data Working Group in collaboration with South East London Save Our NHS. See South East London ICS report: <https://keepournhspublic.com/health-data-working-group/> Appendix 2. [↑](#footnote-ref-2)
2. The ICB Digital Strategy(Draft 2.3.1: July 2023) (Author Martin Wallis, Digital Programme Manager). The Digital strategy was obtained as a pdf in response to an FOI – there is no obvious link to it on the ICB website. [↑](#footnote-ref-3)
3. In situations where it is not deemed possible to gain consent, an application should be made to the Confidentiality Advisory Group (CAG) to consider whether the proposed processing justifies temporarily lifting the common law duty of confidentiality under what’s known as “section 251 support” of the NHS Act (2006) (known as ‘CAG 7-04 (a)/2013). However, this approval only applies to GP, SUS and the Mental Health Services data sets. If other data sets are to be included in RS processing, additional approval must be sought from the CAG. <https://www.england.nhs.uk/wp-content/uploads/2016/10/20220620-Risk-Stratification-Assurance-Statement-v12-3.pdf> [↑](#footnote-ref-4)
4. <https://www.gov.uk/government/publications/letter-to-integrated-care-board-siros-from-the-national-data-guardian-and-uk->

 [caldicott-guardian-council/letter-to-icbs-from-ndg-and-ukcgc-issued-7-november-2022](https://www.gov.uk/government/publications/letter-to-integrated-care-board-siros-from-the-national-data-guardian-and-uk-caldicott-guardian-council/letter-to-icbs-from-ndg-and-ukcgc-issued-7-november-2022) [↑](#footnote-ref-5)
5. Population Health Management has become central to the work of ICSs. The NEL HCP’s Integrated Care Strategy describes the methodology of PHM as “analysing data to identify population cohorts where interventions will add value, [then] intervening, measuring the impact of interventions and incentivising those interventions that add value. It also involves using the data to allocate resources optimally to population cohorts with the greatest need and to interventions that add most ‘value’. (‘data’ is not explained). [↑](#footnote-ref-6)
6. <https://northeastlondon.icb.nhs.uk/wp-content/uploads/2023/08/NHS-NEL-Privacy-notice-risk-stratification-updated-July-2023.pdf> [↑](#footnote-ref-7)
7. According to the Information Commissioner’s Office (the data watchdog), the responsibilities of data controllers include: ensuring compliance with data protection principles; ensuring that individuals can exercise their rights regarding their personal data, ensuring the security of personal data; ensuring the choice of an appropriate processor who is able to guarantee processing meets UK GDPR requirements; entering a binding contract with processors containing compulsory provisions as specified by the UK GDPR; notifying personal data breaches, e.g. to the ICO; complying with GDPR accountability obligations; and complying with GDPR restrictions on transfers of personal data beyond the UK. [↑](#footnote-ref-8)