**The North East London Health and Care Partnership and its use of patients’ data**

**Report by North East London Save Our NHS**

|  |
| --- |
| **SUMMARY**  Integrated Care Systems (ICSs) were introduced in July 2022, fragmenting the NHS into 42 semi-autonomous units. The use of patients’ data is core to the work of ICSs: patients’ personal data informs decisions about direct patient care, and the commissioning and planning of services, including the ‘rationalisation’ of service provision. At the same time, NHS organisations are coming under growing pressure to share their patients’ data for research (both academic and commercial) to help ‘save lives’ through ‘innovation’ and to grow the economy, while legal protections for confidential information are being weakened. It is becoming increasingly necessary to know what ICSs are doing with our data, to ensure good governance and to be able to challenge abuses.  With this in mind, members of the campaign group North East London Save Our NHS (NELSON) submitted a series of Freedom of Information (FOI) questions to the Board (ICB) of the local ICS (the NE London Health and Care Partnership) to look into the way it collected and used patients’ data. The questions were initially based on those developed from research by the KONP Data Working Group in collaboration with South East London Save Our NHS. A number of additional questions were required to follow up initial responses. Questions dealt, in the main with the ICS’s Digital Strategy, its digital governance, its access and use of patients’ health data particularly in Population Health Management and risk stratification. We also asked about the legal bases that the ICS claimed for its use of patients’ data.  The main issues we found concerned the lack of a digital lead on the ICB and a lack of a clear governance structure for the newly formed ICS; poor lay representation on the bodies making decisions about patients’ data; the presence of private company employees on the ICB’s Data Access Group; the embeddedness of private companies; confusion about the use of risk stratification, including a reluctance to share responsibility with providers for informing patients about the way their data may be processed or made use of. It appeared that it was up to patients to find out how their data might be used and the ICB, while happy to use data collected from service providers, did not take steps to ensure the data was collected appropriately. Information also raised concerns about the way that personal data may be used for secondary purposes, and possible lack of compliance with Article 9 (3) of the UK GDPR (requiring all processing of special category data is carried out by a professional subject to a legal duty of confidentiality). Responses also suggested the need for further investigation of Intelligence Solutions for London, which it emerged is a partnership of London ICBs (including NEL) that collectively stores and processes confidential health data.  We conclude that 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. The ICB’s infrastructure for data use is still in flux and its approach to data processing opaque. We suggest that the most effective way of countering the increased access to our data is to continue to monitor what is happening at ICB level and 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. |

**INTRODUCTION**

**The North East London ICS, known as the NEL Health and Care Partnership (NEL HCP), has 2 million residents spread across densely populated inner city areas from Hackney and the City of London in the west to Havering in the east. It is one of the most deprived populations in the country. Over half of the population is from ethnic minority backgrounds, with significant health inequalities existing between ethnic groups.** 70% of the population is struggling in one or more aspects of daily life such as finance, work, food, housing, or loneliness.

The ICS is charged by NHSE with improving disease prevention and healthcare outcomes and ensuring equity of care provision across the population. One of the main ways the ICS is expected to achieve this is through digital transformation and the use of patients’ data.

Responses to FOI requests are presented in six sections dealing with the ICB’s digital strategy; its infrastructure and information governance; the ICB’s use of data; the legal basis drawn on; the involvement of the private sector; and information from data protection impact assessments. FOI questions were largely prompted by concerns about the privacy of personal data[[1]](#footnote-2) and the involvement of the private sector in collecting, storing and processing this data (the names of the private companies that we became aware of are highlighted in green).

**PART ONE: Digital strategy**

**1.1 North East London Health and Care Partnership’s Digital Strategy**

In a foreword to the INEL HCP’s Digital Strategy[[2]](#footnote-3) the CEO of its Integrated Care Board (ICB) stated that digital transformation is key to improving health, tackling rising demand, integrating services, empowering staff and lessening the impact of services on the environment. In addition “This strategy shows how we plan to genuinely co- produce these improvements with our partner organisations and the community across North East London.”

Currently, according to the Strategy:

* Deployment of patient held information is well underway
* The NEL data service is working with Intelligence Solutions for London[[3]](#footnote-4) to form the basis for the London data service layer
* There is good uptake of digitally enabled care and patient information systems (450K eLondon Patient Record accesses per month)
* There is clinical leadership and in-house change capacity for digital transformation
* Funding is secured to move all acute trusts to Oracle Cerner. Both mental health trusts are on Access RiO.

The Strategy suggests a clear push for increased use of a Personal Health Record; and increased virtual interaction with patients, whether this is through the use of video, smart phone or other methods of consultation, or virtual care in the home.

**1.1.2 The Strategic Digital Infrastructure Framework in NEL**

NEL HCP’s focus is to connect IT systems together, minimising the number of different systems in use and utilising the huge amount of data available to inform care both for patients/residents and at population level. The Strategy includes a Digital Infrastructure Framework which provides the following diagram to show the different levels of digital integration:

|  |  |  |  |
| --- | --- | --- | --- |
| **Level 0: Infrastructure/Core Systems** | **Level 1**  **Shared records** | **Level 2**  **Population Health/advanced analytics** | **Level 3**  **Patient access** |
| *Robust foundations & digital maturity* | *Single patient record* | *Realtime information for proactive care*  *Using population information* | *Patient empowerment* |
| The fundamental basis for all digital activity; the foundational work done at each provider allowing them to operate effective and work with external systems. These systems include end user devices, electronic patient record systems, network capacity, cyber security etc in all care settings including community diagnostic centres and care sector. | For care professions in social care departments, Trusts, GP, care homes, hospices, community pharmacists and other care settings. Primarily provided through the east London Patient Record (eLPR) and related London Care Record. | Uses variety of data sources to build picture of care needs at various levels, primarily identifying specific cohorts of patients needing intervention but also providing overviews at population level, allowing providers to alter service provision. Primarily provided via the Data Discovery Service plus additional data sets and capacity planning systems eg Edenbridge Healthcare [[4]](#footnote-5) | Provided through expanding the use of the NHS App, on-line and video consultation tools, on-line registration and the patient held record system, Patients Know Best. |
| Key strategic programmes are co-ordinated by the ICS team, including Community Diagnostic Centres, Frontline Digitisation, Virtual wards, Care Sector, secondary care Appointment Systems and Primary Care Digital First, working with health, social care and third sector partners |  | Patient level and aggregated information provided via the Discovery Data Service (and other sources) to clinicians, managers and researchers, subject to a strict approval process. This helps change pathways as well as the planning and delivery of healthcare provision across NEL, NWL & SEL. |  |

NE systems, CEG facilitators focussing on the use of data and IT facilitators focussing on

The Digital Strategy also outlines a draft digital roadmap for 2023/4 and 2024/5 (see Appendix 1), which (among other things) indicates that Patients Know Best (with Sectra[[5]](#footnote-6) and EMIS,[[6]](#footnote-7) the only other private companies mentioned) is integral to the strategy. The explanation is that ”The collaborative implementation of PKB across the ICS will see significant improvement in DMA [Digital Maturity Assessment for Government][[7]](#footnote-8) score over the next two years”.[[8]](#footnote-9)An overview of the ICS’s digital maturity notes 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 a lack of a clear governance structure while the ICS forms.

**PART TWO: Infrastructure and information governance**

**2.1 The NEL ICB Governance Handbook**

Given the significance that the ICB gives to digital transformation, the NEL ICB Governance Handbook makes only two references to data (and digital). The first is to a responsibility of the ICB to lead on system-wide action on data and digital. The second reference concerns establishing a shared approach to population health “with an approach to data and the digital infrastructure to support this, and enable us to tackle inequalities”.[[9]](#endnote-2)

In outlining the work of the ICB’s committees, the Handbook includes Terms of Reference (ToR) for its Audit and Risk Committee, but this only mentions data in terms of its security (with no reference to digital) while, surprisingly, the ToR for the Population Health and Integration Committee make no mention of data (or digital) at all.

**2,2 Information Governance Framework (IGF)**

This Framework[[10]](#endnote-3) provides the basis upon which data protection and information governance (IG) and all its component parts will be implemented throughout NEL ICB. It outlines the roles and responsibilities of those tasked with ensuring that IG is appropriately supported, that necessary guidance and advice are available in an effective and efficient manner, and the responsibilities for all staff are clear.

The Framework emphases that the law allows personal confidential data to be shared between those offering care directly to patients, but it protects patients’ confidentiality when data about them is used for other purposes. However it asserts that these “secondary uses” of data are essential to run a safe, efficient, and equitable health service. Purposes include: reviewing and improving the quality of care provided; researching which treatments work best; commissioning clinical services; and the planning of public health services.

The Framework refers to an Information Governance Steering Group and a Data Access Group (neither of which are mentioned in the Governance Handbook).

**2.3 The Information Governance Steering Group (IGSG)[[11]](#endnote-4)**

The IGSG has delegated authority from the Governing Body to oversee operational work and workplans across the information governance agenda, acting as a focal point for the reporting, investigation, and response to information incidents, supporting the Caldicott function and acting as the Records and Information management group. The IGSG oversees the work of a Data Access Group (see below).

An FOI response stated that the ToR for the Information Governance Steering Group were not yet agreed. However the Information Governance Framework says that the IGSG submits its minutes, work plan and action points to the Integrated Governance and Performance Committee (of which we could find no trace) once approved. It also provides assurance to the ICB’s Audit and Risk Committee on the structure and effectiveness of data protection and information governance controls within the organisation.

An FOI response stated that the IG Steering Group does not include representatives from private companies, and that members are required to keep a conflict of interest register should any hold external positions. There is no patient or public representation – a question asking why this was the case was unanswered as it was deemed inappropriate for an FOI request.

**2.4 Data Access Group (DAG)**

The DAG oversees the lawful sharing of personal data and other corporate data by all relevant parties across the ICS geography. It considers requests and makes recommendations to approve (or not approve) data sharing, and provides assurance (and evidentiary documentation) for system partners that all relevant and proper checks are considered prior to data sharing. It also carries out Data Protection Impact Assessments (DPIA) and Digital Technology Assessment Criteria (DTAC) reviews as needed and implements all relevant legal and good practice documents such as Data Processing Agreements and Data Sharing Agreements.

Being an ICS-wide, multi-agency group, the DAG is not in itself an approval authority, although its membership does consist of relevant technical experts from ICS system partners. Instead, the DAG makes recommendations to the ICB IGSG for final approval. The group does not routinely publish its minutes or other documents and it has no lay members.

Membership of the DAG as listed in April 2023 was dominated by ICB members, and otherwise included representatives from the ICS’s Trusts, some GP practices and LAs, plus two ‘independent’ members: Nick Murphy O’Kane (employed by KNG Plus Consultants, who appear to deal with information governance, data analysis, security and training) and Miles Dagnall (Consultant with JEM GDPR Consultancy, specialists in IT). It is unclear why representatives from private companies are allowed seats on the ICB’s decision-making body for data access.

The NEL ICB recently released a new data sharing framework for the North East London ICS geography. The current ICB Data Access Group will be re-formulated under this new framework. When the new groups managing this framework across the ICS are constituted, they will agree terms of reference. One of the proposals for the new framework is to consider lay representation on the reformulated group and when constituted, they will consider this matter alongside the new terms of reference.

**ensuring practice systems are usable. Trusts provide their own training for staff.**

**PART THREE: The ICB’s use of data**

**3.1 Access to patients’ data**

By 2022, 95% of the ICS’s original five boroughs had signed up to the Discovery East London service,[[12]](#footnote-10) a scheme described by the ICB as allowing clinicians in mental health services and hospitals (and other services to follow) to see summarised patient records, such as diagnosis and medications. Information provided by Discovery is also used “to understand what local populations need”. For example,

“In Tower Hamlets, anonymised health care datasets have been combined with ‘socio-economic patterns’ – information on where, and how people live and work – to map deprivation and morbidity outcomes across the borough. This means we have a much clearer understanding of health outcomes and we can use this information to decide where to allocate resources. We also share the data with the National Cancer Registry, contributing to applied research on cancer care.”

We put a question to the ICB asking how access to patients’ confidential data was being governed so that the public could have confidence in the way their personal data was being used by the ICS. The answer was that, as established by the UK GDPR, data controller responsibilities[[13]](#footnote-11) always rest with individual controller organisations (ie care providers such as GPs or hospital Trusts) that collect data, and neither the ICB nor ICS can overrule this. *The ICB therefore depends on the data collected by the organisations within it but it takes no part in ensuring the integrity of the data collection processes of these organisations.*

Similarly, asked how the ICB ensures independent oversight of the way organisations within the ICS use confidential patient information, the response was phrased in terms of the Data Access Group’s (DAG) responsibilities. It said that “the group is open to all parties within NHS NEL ICS to ensure that all partieshavescrutiny of proposed projects from a data protection / information governance perspective before each organisation approves.” The point is made that the DAG has no authority over individual controllership but “exists to facilitate appropriate input to proposed projects from a data protection/ information governance perspective”. In other words, *the ICB has no responsibility for how the organisations within it process and share the patient information for which they are controller.*

Asked what arrangements were 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 privacy notices could be found, we were referred to the websites of the ICB and ICS, which provided details of the providers across the ICS. *Expecting patients to scour the ICS website for providers and then the websites of those providers to see a privacy notice that they may 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”.

**3.2 The use of patients’ data**

The main ways that the ICB says that it uses patient data are

a) using anonymised and aggregated data to plan healthcare services, e.g. for checking service quality or predicting future service needs, and

b) using pseudonymised (de-identified) information for commissioning services and risk stratification.[[14]](#endnote-5)

The ICB’s Annual Report (2022-2023) makes brief reference to how data and digital infrastructure supports population health, with population health management one of the ICB’s key priorities.[[15]](#endnote-6)

**3.2.1 Population Health Management (PHM)**

The NEL HCP’s Integrated Care Strategy notes that Population Health Management, used in the planning and delivery of services, is being used to support a greater focus on prevention.[[16]](#endnote-7) The Strategy describes PHM as “A focus on improving physical and mental health outcomes, promoting well being and reducing health inequalities across an entire population, including a specific focus on the wider determinants of health (such as housing, employment and education”.

PHM is widely promoted as a way of changing the behaviour of people within a defined population (not just those in direct contact with health or care services) and who are at risk, for example, from modern epidemics such as obesity. However, the multinational corporation Deloitte throws a different light on PHM, suggesting it is about data analytics, financial risk and cutting costs; realigning funding flows; facilitating new payment systems, with most funding becoming population based; and allowing new (financial) incentives and performance metrics to ‘encourage’ staff to work differently across different settings.[[17]](#endnote-8) The NEL HCP’s Integrated Care Strategy hints at this interpretation by emphasising the use of PHM to determine ‘value’:[[18]](#footnote-12) it describes the methodology of PHM as

“analysing data to identify population cohorts where interventions will add value, 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.”[[19]](#footnote-13) [[20]](#footnote-14)

PHM uses linked datasets, combining healthcare and non-healthcare data from a variety of sources including government, local authorities and social services (e.g. lifestyle, housing, and deprivation data).  In response to questioning, the NEL ICB explains that PHM involves segmenting a population into groups based, for example, on similar health issues (such as diabetes, or frailty,) and ‘impactability modelling’ to identify ‘at risk’ cohorts (see ‘Risk Stratification’ section below). This in turn leads to the design and targeting of interventions to prevent ill health and hospital admissions and improve care and support.

Asked how the ICB – as required under the UK GDPR - was ensuring that individuals were made aware *at the point when their data was collected* about how their data was going to be *processed* for purposes such as PHM, the response was familiar: “In general, the ICB rarely originates the data. Commissioned care providers[[21]](#footnote-15) obtain the data and they have an obligation to inform data subjects about the proposed processing”. It added that “In general, the role of an ICB whilst determining the purpose and manner of processing for Population Health Management share the obligations with the data source via the contracting process.[[22]](#footnote-16) This answer ignores the fact that if patients’ data is going to be used for risk stratification (see below), the ICB and GPs (or their risk stratification suppliers) only have a lawful basis for this if they meet certain conditions, including ensuring that the public understand the proposed use of their data for these purposes.

Questioned about the data sets used by the ICB and linked for PHM purposes, the response was that

The data includes commissioning flows such as SUS (Secondary Uses Services),[[23]](#footnote-17) MHMDS (Mental Health Services Data Set), CDS (Commissioning Data Sets), MSDS (Maternity Services Data Set), ECDS (Emergency Care Data Sets), 111, Ambulance. Patient level data sets are pseudonymised and linked to Primary Care data to provide a holistic view of health activity. In addition, publicly available datasets that provide important context to activity are used in analysis (e.g. particular, pollution levels, weather). Data sharing frameworks are currently being put in place to facilitate the flows of local authority data such as Adult Social Care. The ICB will explore other local authority data sets as the use cases for sharing data are developed.

Further responses referred additionally to data extracted from SystmOne[[24]](#footnote-18) and EMIS (hosted on Amazon Web Services servers), Diagnostic Imaging Data Set (DIDS) and Community Services Data Set (CSDS), plus national indicators and benchmarks via the Office for Health Improvement and Disparities’ (OHID) ‘Fingertips’[[25]](#footnote-19)and the use of demographic projections from the Office for National Statistics and the Greater London Authority to support the understanding of population need and ‘areas of opportunity’ to address inequalities.

In response to a question about the data that the Population Health and Information Governance Steering Group collects, it became clear that the ICB’s Primary Care and commissioning data are patient level but pseudonymised[[26]](#footnote-20) “in line with the anonymisation rules as outlined by the ICO”. This raises two points:

i) what counts as anonymous data (and thus beyond data protection legislation) will become far more subjective if the Data Protection and Digital Information Bill is passed; and

ii**)** PHM is reliant on aggregating a range of data sets. One implication is that, even if personal data is pseudonymised, the more that data is linked[[27]](#footnote-21) at an individual level, the greater the probability there is of identifying individuals. This poses the question of *how closely those who are using patients’ personal data are complying with data protection legislation*.

**3.2.2 Risk stratification**

Among its methods, PHM uses risk stratification to identify groups and, potentially, individuals who might benefit from interventions: it’s suggested that

At the individual level, a patient's risk category is the first step towards planning, developing, and implementing a personalised care plan. One common stratification method is to segment patients by “risk” level: high-, medium- (rising), and low- risk. At the population level, risk stratification allows care models to be personalised to the needs of patients within each subgroup.[[28]](#endnote-9)

Risk stratification may have the potential to improve care quality (for some) while reducing costs but NHSE[[29]](#endnote-10) has also clarified that it can be beset by problems. Risk stratification tools are never entirely accurate and have the potential to provide false positive and false negative results, with adverse effects. Additionally, some adjunct tools (‘impactability models’) used to improve the efficacy of risk stratification may worsen health inequalities. Preventive interventions offered in risk stratification programmes may be based on little evidence and potentially increase rather than reduce total costs. Additionally, a risk stratification approach prevents valuable continuity of care with a skilled member of the clinical team as patients may not be seen until they reach a predetermined risk threshold.

In response to a FOI question in March 2023 (and despite acknowledging in a different FOI response that using PHM involved ‘impactability modelling’ to identify ‘at risk’ groups) the ICB stated that it was not currently using data for risk stratification and therefore it could not provide the Risk Stratification Assurance Statement we requested. Instead of risk stratification, we were told that PHM involved data linkage that was not outsourced but carried out by ICB staff to support ‘case findings’ for patients (see Section 3.2.3 below for more on staff).

Having said that, the ICB’s Privacy Policy (July 2023)[[30]](#endnote-11) provides a link to a Privacy Notice specifically concerning “Risk Stratification for Case Finding” that states

“Your GP uses your data to provide the best care they can for you. As part of this process, your GP will use your personal and health data to undertake risk stratification, also known as case finding.

Risk stratification involves applying computer-based algorithms, or calculations, to identify those patients registered with the GP Surgery who are most at risk from certain medical conditions and who will benefit from clinical care to help prevent or better treat their condition.

To identify those patients individually from the patient community registered with your GP would be a lengthy and time-consuming process, which would by its nature potentially not identify individuals quickly and increase the time to improve care.

NEL will automatically process your personal and confidential data without any staff being able to view the data. Typically, they will process your data using indicators such as your age, gender, NHS number and codes for your medical health to identify those who will benefit from clinical intervention.[[31]](#endnote-12)

The Notice identifies the data controller as ‘Your GP” and the data processor as NHS North East London (an alternative name for the NEL Health and Care Partnership.[[32]](#footnote-22)

In sum, responses from the ICB appear to suggest confusion about whether or not it carries out risk stratification. When it denies that risk stratification is used it says that, instead, it carries out case finding. However, the ICB’s Privacy Notice suggests that risk stratification is a necessary prelude to case finding.

In response to an FOI asking how the ICB is carrying out Population Health Management without doing Risk Stratification (e.g. what method is being used to identify individuals or groups who would benefit from interventions), we had the following reply:

“No one specific risk stratification algorithm is applied in our linked data set. There are basic Clinical Prediction Models (CPM) applied to the data on SUS only data, e-frailty scores. In addition, patient facts have been developed, coded and derived from the coded clinical data to determine if patients have or are ‘smokers’, ‘obese’,’ diabetes’, ’learning disabilities’ ‘SMI’ and other value sets driven from clinical and demographic details – deprivation, living with multiple co-morbidities. Through the development of curated data models certain patient ‘segments’ are derived – Healthy, Living with Cancer, acute LTCs, maternity, end of life. Analysis is undertaken on *utilisation and cost of services* looking at our core 20 population[[33]](#footnote-23) as an example. CPM provides a crude risk of admission score. As part of our development and maturity the ICB will be looking at risk algorithms adoption and the application of 3rd party vs internally developed segmentation models”.

Overall, this kind of analysis develops profiles or scores to identify potentially high cost patients. One implication of the current approach is that there is no need to identify individual patients to do this analysis (and therefore no need to rely on ‘Section 251 support’ - see below).

**3.2.3 Risk stratification, consent and confidentiality**

Recently, the National Data Guardian and UK Caldicott Guardian Chair of Council (NDG & CCC) jointly expressed concern that, within some data sharing programmes, organisations were using confidential patient information (CPI) for purposes other than direct care without ensuring that their activities did not breach confidentiality.[[34]](#endnote-13) They emphasised, for example, that the secondary use of GP and SUS data for *processing* purposes (in contrast to direct care purposes) cannot rely on implied consent. Instead, organisations have to justify processing. For example, 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).[[35]](#footnote-24)

This is particularly relevant to the preliminary combining and processing of confidential patient information (CPI) for risk stratification purposes. In 2013 NHS England gained approval from the Secretary of State (through CAG) for data processors working on behalf of GPs and Clinical Commissioning Groups (CCGs) to have access to SUS, commissioning data sets and GP data for risk stratification purposes. However, as mentioned earlier, approval is conditional: for example,

* NHSE must seek assurance from ICBs and their appointed risk stratification suppliers that data processing is in accordance with the Data Protection Act (2018), and provide a register of organisations[[36]](#footnote-25) approved for the receipt and processing of patient data for risk stratification.
* ICBs and GPs only have a lawful basis for data use if they (or their risk stratification suppliers) meet conditions set out in a Risk Stratification Assurance Statement.[[37]](#footnote-26) This should include ensuring that
  + the public understand proposed use of data for risk stratification purposes.
  + risk stratification suppliers receive “de-identified data for limited access” (or data pseudonymised ‘on landing’); data is processed in a closed box with strict role-based control and to a standard that minimises the use of patient confidential data.
  + re-identification of data is solely for the purpose of direct care and available only to those with a direct care relationship to the individual.

We submitted an FOI requesting a copy of the ICB’s Risk Stratification Assurance Statement and a link to their register of approved organisations but were told in response that the ICB did not carry out risk stratification. They did say however in a different response that the London ICSs *as a group* were not extracting more data to risk stratification systems than originally approved under CAG 7-04(a) 2013, and *were not using organisations to do risk stratification that were not on the list approved to receive and process confidential patient information.* The response went on to say “in fact in truth these Risk Stratification systems are not really being used at all any more”. Moreover, the London ICSs were

“working closely together to develop our approach to Population Health Management and we will not be relying on the NHS England section 251 support in CAG 7-04(a) 2013, nor the tools that grew from that Risk Stratification programme to support this work”.[[38]](#endnote-14)

One point to pick up from this is that it seems that while London ICSs (including NEL) are, as a group, extracting data and carrying out risk stratification (in accord with CAG 7-04(a) 2013) and using organisations on an approved list to do so, the ICB maintains it is *not* carrying out risk stratification and only uses in-house staff for data processing. This suggests that the NEL ICB does not consider itself to have any responsibility for what is done in its name at arms length.

A further FOI asked how the ICB was addressing NDG and CCC concerns about the disclosure of confidential patient information outside the shared care record team/systems to render it anonymous for secondary purposes. The response was that

This concern seems to centre on using 3rd party suppliers or organisations to anonymise data held in shared care records or Risk Stratification tools and sending them confidential patient information to support this work. The London ICSs are not using 3rd party suppliers or organisations to do this work with their shared care record nor with its Risk Stratification tools.

This response appears to be contradicted by the information in a Data Impact Assessment considering the potential introduction by NEL of Eclipse, a medications prescription risk stratification tool that collects personal data (see below).

Asked whether the ICB complied with Article 9 (3) of the UK GDPR and ensured all processing of special category data was carried out by a professional who was subject to an obligation of professional secrecy or legal duty of confidentiality, there was no clear answer: we were told that all staff working on such data hold NHS employment contracts with the relevant codes of practice around confidentiality and have up to date training on Information Governance. This suggests that the ICB may not comply with Article 9 (3) of the UK GDPR.

On a related theme, in response to a question about the role of Place Based Partnerships in providing data to the ICB for PHM, we were told that

*“*The NEL ICB Intelligence and Insights function are committed to supporting Population Health Management and they will work with providers and public health analysts when sharing arrangements allow collaborative working”.

We followed up this question by asking more about private providers’ responsibilities associated with data collection for the ICB’s intelligence and insights function, in particular what measures were in place to ensure that private providers do not use patient data for their own purposes. The response was

“Where a private provider (3rd party) are used to support data collection or curation of data for the ICB then they would be doing so under contract and under instruction from data controllers. Any private provider therefore will be subject to the confidentiality terms and conditions that will guide against unlawful processing activities.”

*I*t is unclear how or whether compliance with the conditions of contracts with private providers are monitored*.* If this is the responsibility of data controllers such as GPs, it is hard to imagine that they have the resources to carry out this work.

**PART 4: Lawful basis and the nature of the data used**

Asked about the nature of data made available to the Population Health Plans referred to by the ICB (plans we have since been unable to get hold of), the response was that as these plans only intend to use anonymised and not confidential data, they are not subject to the UK GDPR or the Data Protection Act 2018. The ICB therefore does not need to rely on consent as a lawful basis. Confidential personal data would only ever be used for population health where there is a clear, lawful basis to do so as described by UK GDPR.

However, when asked about the legal basis for accessing and processing confidential patient information used for identifying vulnerable or individuals at risk and those who might benefit from targeted interventions, the response was “that this would depend on the proposed processing action. Moreover,

“Whilst the ICB may have access to identifiable data, the proposed processing has privacy controls and access restrictions and pseudonymised data is used to limit re-identification for those with a lawful basis and legitimate clinical relationship. However, in general the proposed processing would usually fall under one of these statutory obligations on an ICB:

* + Duty to improve the quality of services. (HSCA 2012, s26).
  + Duty to reduce inequalities (HSCA 2012 s26).
  + Duty that each ICB whilst carrying out its functions must have a regard to the need to reduce inequalities between patients with respect to their ability to access health services, and reduce inequalities between patients with respect to the outcomes achieved for them. In order to facilitate this, it is necessary to undertake geographical analysis based on postcode. (NHS Act 2006 s14T).
  + Duty to exercise its functions effectively, efficiently and economically. (HSCA 2012 26).
  + Duty to secure continuous improvement in the quality of primary medical services (HSCA 2012 s26).”

These statutory obligations allow the ICB to claim very broad powers under the UK GDPR to process confidential personal data, such as in the delivery of risk stratification, namely:

* GDPR Article 6(1)(e) – ie processing is necessary for the performance of a task carried out in the exercise of official authority vested in the controller.
* GDPR Article 9(2)(h) = ie 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.

The ICB’s Privacy Notice also states that where processing is “necessary to perform a task in the public interest” and “for a medical purpose”, individuals’ right to have their personal data erased, as set out in the GDPR, is not applicable.

**PART 5: Private company involvement in data collection or curation for the ICB**

We did not ask specific questions about the private companies involved in data collection or curation. Such involvement did not usually emerge in responses to the questions we asked, but became more apparent when combing through ICB documents, such as risk Data Protection Impact Assessments. There was a sense that, the more one looked, the more companies would emerge. To confirm the extent of this embeddedness requires further investigation.

**PART 6. Data Protection Impact Assessments**

Data Protection Impact Assessments provide a way of assessing the risks posed by a proposed activity involving the processing (including the collection, structuring, dissemination, destruction, or storing) of personal data. An FOI requesting impact assessments by all relevant data controllers involved in the ICB’s population health management activities prompted just two responses. These are included here because they give a glimpse of how patients’ data is being used, the involvement of private companies and because one example suggests the continuing use of risk stratification.

***6. 1. Eclipse***

The Impact Assessment dated January 2023, concerns the proposed use of Eclipse,[[39]](#footnote-27) a risk stratification tool in the process of being implemented across the ICS primarily for medicines management. This will connect SUS with GP patient data. The service will involve new or the significantly changed handling of a considerable amount of personal or special category data about each individual from multiple sources, justified on the basis that identification of patients is key to enabling the direct care i*n the event of ‘case finding’*. The personal data collected will be the patient’s name, address, postcode, NHS number, email address, date of birth, and the special category data will be racial/ethnicity and physical/mental health information.

The processing is said to conflict with other agreements to which data controllers are party, but in what way or what the implications of this conflict might be are not enlarged upon. The data will be de-identified using the NEL Pseudonymisation tool. of which we have no details.

The legal basis given for processing identifiable data is GDPR Article 6(1)(e) – (see above), and for processing special category data is GDPR Article 9 (2)(h)(again, see above). This lawful basis means that the right to erasure is not applicable. There is no mention of what happens if patients have opted out.

***6.2. Snowflake***

Previously the NEL CCG (replaced by the ICB) held commissioning data on two platforms – one provided by the Commissioning Support Unit and Data Services for Commissioners Regional Office (DSCRO) (based on data from local providers such as GP practices) and a separate Microsoft Azure platform that was managed by NEL. A data cloud called and apparently provided by Snowflake [[40]](#endnote-15)and deployed on AWS, allows the data from the two platforms to be combined and processed.[[41]](#endnote-16) The service is provided on a ‘pay as you go’ basis: clients only pay for what they use and are charged on the basis of per-second pricing.

Population health and demographic information is all pseudonymised (although it is not clear who by) without NEL CCG nor Snowflake having access to any keys to re-identify it. Rather differently, data from DSCRO is provided pseudonymised by the CSU. The personal data includes postcode (truncated to just outbound code), date of birth, gender, ethnicity, local identifiers (a GP reference) and special category data used relates to health – all pseudonymised data.

The legal basis claimed for processing is given as GDPR Article 6 9(e) and GDPR Article 9 2 (h) (as above), and additionally by GDPR Article 9 2 (I) (Necessary for reasons of public interest in the area of public health). Again, individuals’ rights of data erasure do not apply. The Common Law Duty of Confidentiality is satisfied on grounds of ‘public interest’ and ‘legal obligation’.

The Impact Assessment confirms that identifiable data cannot be used for secondary purposes where the patient has opted out, but pseudonymised data can be used without obtaining a patient’s consent. The National Data Opt Out only applies to approved S251 research: as Snowflake processing is not subject to this approval, the national opt-out does not apply. [[42]](#endnote-17)

**CONCLUSION**

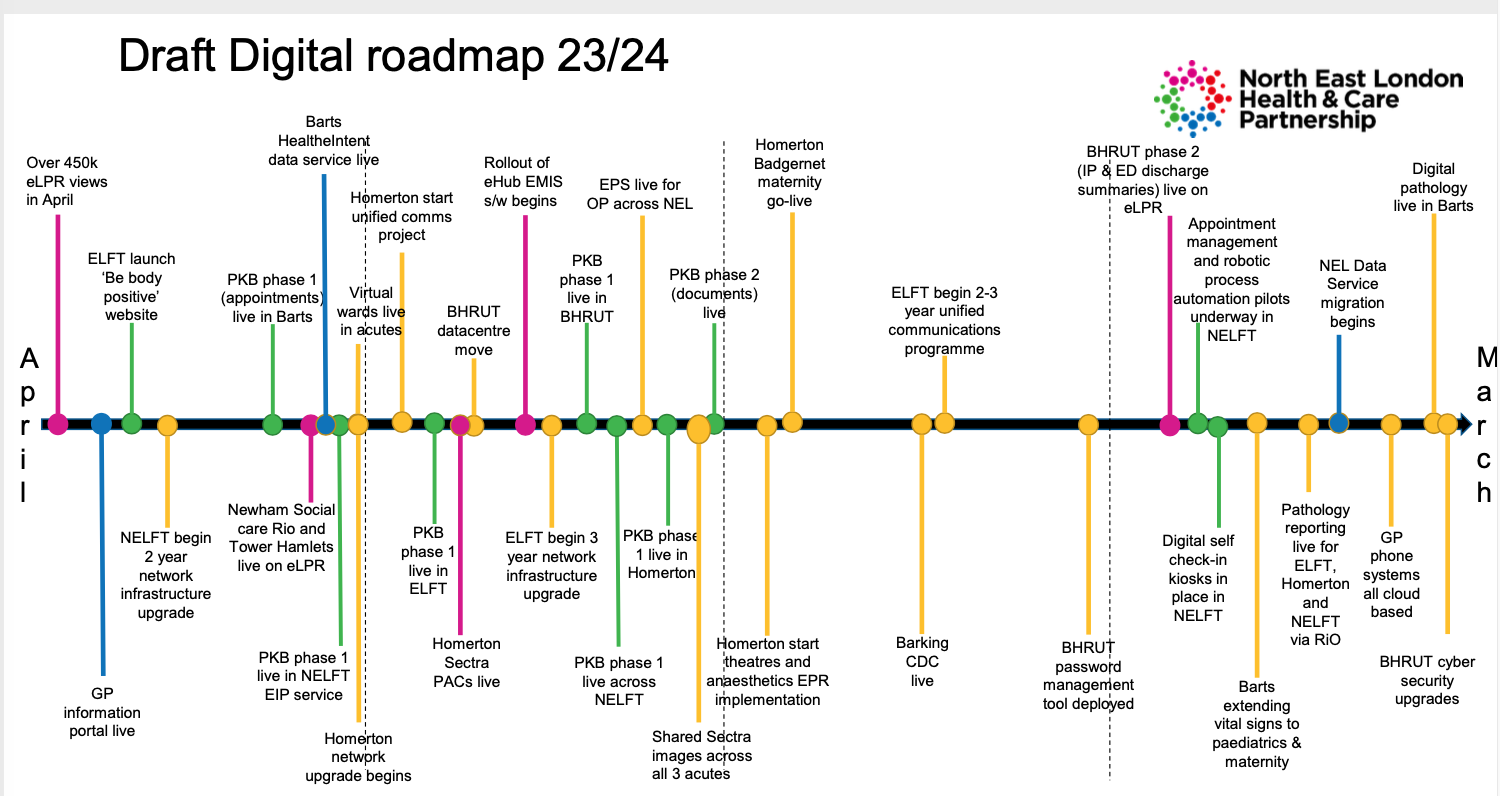
Responses to our FOI enquiries suggest that the ICB is under pressure to achieve digital transformation at pace and is struggling to set up the infrastructure for data governance that should underpin its use of patients’ data. Its approach to data processing is opaque. In particular, it was unclear whether or not the ICB was carrying out risk stratification as part of its use of Population Health Management. The ICB also seemed to assume little responsibility for the data it relied on, for example whether it was collected appropriately, with measures in place to ensure patients knew about the collection and use of their data. There was also poor lay representation on the bodies making decisions about patients’ data. We were concerned to see the presence of private company employees on the ICB’s Data Access Group and were given little reassurance about whether or not private companies under contract to process patients’ data would be prevented from using this for their own purposes.

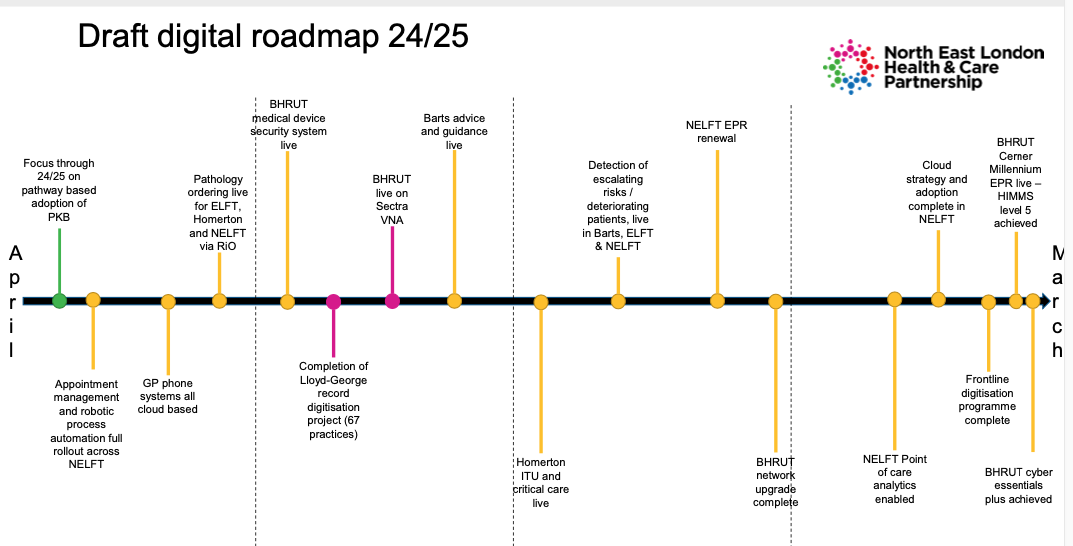
Legislation already provides the ICB with huge scope for accessing and processing personal data, while forthcoming legislation is only likely to weaken existing data protections. In addition, the Department of Health and Social Care/NHSE are introducing a system of ‘data access as default’ for the secondary uses of NHS health and social care data facilitated by the implementation of Secure Data Environments. It is unclear at the moment how much this will change the way ICB’s access patients’ data in future or what the legal implications will be. At the moment, we can only guess that protections for our data will diminish further.

We suggest that the most effective way of countering the increased access to our data is to continue to monitor what is happening at ICB level and demand accountability and transparency on the part of those using our data, not least through providing public access to relevant committees and their papers, while insisting on the data protections that we still have.

Appendix 1.

Draft Digital Roadmap





1. Article 4 of UK GDPR defines ‘**personal data**’ as any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. [↑](#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. ISL is part of a partnership arrangement for 5 London ICBs. The team delivers services across data warehousing and engineering, analytical solutions, design and implementation, delivery assurance and support. [↑](#footnote-ref-4)
4. Edenbridge provides business intelligence tools to GPs, other providers and commissioners. Their product Apex, which “delivers IT solutions at scale to the Primary Care market” has been bought by EMIS. [↑](#footnote-ref-5)
5. Sectra, a multinational, develops and sells solutions in medical IT and cybersecurity [↑](#footnote-ref-6)
6. EMIS has been the dominant Electronic Health Record vendor for NHS GP practices and also leads the UK community pharmacy IT, inpatient EDIS and community EHR markets, as well as providing providing booking management systems and a virtual care platform for many primary care practices via its Patient Access business. The acquisition of EMIS by Optum (a company owned in turn by US insurance and healthcare IT giant UnitedHealth) has been described as ‘monumental’. Both EMIS and Optum are listed as authorized vendors under the HSSF. [↑](#footnote-ref-7)
7. DMA or Digital Maturity Assessment for Government aims to help public sector organisations measure, improve and maintain the health and strength of their data ecosystems. <https://www.gov.uk/government/collections/data-maturity-assessment-for-government> [↑](#footnote-ref-8)
8. PLK is currently contracted for more than 12 million people to use its service across the UK. PKB **states that it is the only provider of personal health records able to offer patients their combined information, in association with the NHS App. This integration, underpinned by NHS login, allows users of the NHS App to directly sign up for a PKB record to enhance the App’s current offering of access to GP records only, and “empower[s] patients to have greater visibility and ownership of their own medical records”. Plus patients are told that the more data that they add (eg health diaries) the more useful their PKB record will be for clinicians.**  [↑](#footnote-ref-9)
9. REFERENCES

   i <https://northeastlondon.icb.nhs.uk/wp-content/uploads/2022/11/NELICB-Governance-handbook-v7.pdf> [↑](#endnote-ref-2)
10. Information Governance Framework https://intranet.northeastlondon.icb.nhs.uk/wp-content/uploads/2023/07/FRW-

    [IG-01-NEL-ICB-IG-framework-July-2022-1.0-Final.pdf](https://intranet.northeastlondon.icb.nhs.uk/wp-content/uploads/2023/07/FRW-IG-01-NEL-ICB-IG-framework-July-2022-1.0-Final.pdf) (September 2022) [↑](#endnote-ref-3)
11. <https://intranet.northeastlondon.icb.nhs.uk/wp-content/uploads/2023/07/FRW-IG-01-NEL-ICB-IG-framework-July-> [2022-1.0-Final.pdf](https://intranet.northeastlondon.icb.nhs.uk/wp-content/uploads/2023/07/FRW-IG-01-NEL-ICB-IG-framework-July-2022-1.0-Final.pdf) [↑](#endnote-ref-4)
12. DDS hosts the London Care Record, a view-only source of data under One London control and governance, and accessible only by those involved with the direct care of patients. In addition, but separately, the DDS hosts the individual population databases of its three founding ICSs (North East London, North West London and South East London), providing a data environment that can be accessed for clinical research, quality and care improvement, health and care commissioning, population health management and “cross care-setting innovation” (presumably meaning integrated service re-design), subject to data sharing agreements, consent and satisfactory security arrangements. [↑](#footnote-ref-10)
13. 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-11)
14. <https://northeastlondon.icb.nhs.uk/privacy-policy/> [↑](#endnote-ref-5)
15. <https://northeastlondon.icb.nhs.uk/wp-content/uploads/2023/07/ICB_Annual_Report_2022-23_FINAL.pdf> [↑](#endnote-ref-6)
16. <https://www.northeastlondonhcp.nhs.uk/wp-content/uploads/2023/05/NEL-Interim-integrated-care-strategy-31-January-2023-final.pdf> [↑](#endnote-ref-7)
17. [management.pdf](https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/public-sector/deloitte-uk-public-sector-population-health-management.pdf) [https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/public-sector/deloitte-uk-public-sector-population-health-](https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/public-sector/deloitte-uk-public-sector-population-health-management.pdf) [↑](#endnote-ref-8)
18. 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-12)
19. It is worth noting that the approval NHSE received for processing personal data for risk stratification expired in September 2023. [↑](#footnote-ref-13)
20. What is meant by data is not spelt out. [↑](#footnote-ref-14)
21. Presumably meaning GP practices, NHS Trusts etc. [↑](#footnote-ref-15)
22. Presumably meaning data sharing agreements between the ICB and GP practices, NHS Trusts etc. but also with processor contracts as ICB is responsible for ICS wide commissioning. [↑](#footnote-ref-16)
23. SUS collects anonymous, patient-level data for purposes beyond direct care such as healthcare planning, medical research, national policy development. [↑](#footnote-ref-17)
24. SystmOne is a single Electronic Health Record allowing clinicians to access and contribute information about a patient across a wide variety of health settings, during the patients’ care. <https://tpp-uk.com/products/> [↑](#footnote-ref-18)
25. The OHID works across the Department of Health and Social Care, the rest of government, the healthcare system, local government and industry ‘to be creative’ about how their focus shifts towards preventing ill health, particularly where there the most significant disparities. Fingertips is their web-based platform providing easy access to a rich source of indicators across a range of health and wellbeing topics [https://fingertips.phe.org.uk](https://fingertips.phe.org.uk/). [↑](#footnote-ref-19)
26. Pseudonymisation removes most identifying elements within a data record, and replaces these with artificial identifiers or pseudonyms. Notably, this process does not change the status of the data as personal data and it is still covered by the requirements of the GDPR. [↑](#footnote-ref-20)
27. Data linkage is described by the ICS as bringing together information held by different organisations such as NHS Trusts primary care and local authorities to allow clinicians and planners to better understand the needs of the population, including the wider determinants of health. <https://www.northeastlondonhcp.nhs.uk/wp-content/uploads/2023/05/NEL-Interim-integrated-care-strategy-31-January-2023-final.pdf> [↑](#footnote-ref-21)
28. <https://www.sectorsupportnel.org.uk/wp-content/uploads/2022/11/PHM-in-NEL-091122-GB2.pdf> [↑](#endnote-ref-9)
29. https://www.england.nhs.uk/wp-content/uploads/2015/01/nxt-steps-risk-strat-glewis.pdf [↑](#endnote-ref-10)
30. <https://northeastlondon.icb.nhs.uk/privacy-policy/> [↑](#endnote-ref-11)
31. <https://northeastlondon.icb.nhs.uk/wp-content/uploads/2023/08/NHS-NEL-Privacy-notice-risk-stratification-updated-July-2023.pdf> [↑](#endnote-ref-12)
32. A previous version of the Privacy Notice (now disappeared) gave the data controller as the NEL. It also suggested that risk stratification is additionally used to support decisions about the funding of treatment: “This data is used to assess whether you meet the criteria for funding for these services and to enable provision of services thereafter”, but this information has disappeared on the updated version. It is tempting to think that the revised Privacy Notice is in response to some of the FOIs from campaigners. [↑](#footnote-ref-22)
33. *Our* Core 20’ appears to refer to Core20Plus 5: The approach defines a core target population – the most deprived 20% of the national population; ‘Plus’ refers to population groups identified by the ICB as experiencing poorer than average health access, experience and/or outcomes not necessarily captured within Core 20 alone; and ‘5’ – the clinical areas identified nationally as requiring accelerated improvement. <https://www.england.nhs.uk/about/equality/equality-hub/national-healthcare-inequalities-improvement-programme/core20plus5/> [↑](#footnote-ref-23)
34. <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) [↑](#endnote-ref-13)
35. CAG 7-04 (a) 2013 allows preliminary processing to combine and process specific primary and secondary care data to identify vulnerable or high risk patient populations who may be suitable for interventions. [↑](#footnote-ref-24)
36. Only named and existing risk stratification suppliers and existing contracts listed in the latest version of the Risk Stratification register on the NHSE website are eligible to provide risk stratification services under the conditions set out in CAG 7-04(a)/2013. <https://www.england.nhs.uk/publication/list-of-risk-stratification-approved-organisations/> [↑](#footnote-ref-25)
37. It is worth noting that the approval NHSE received for processing personal data for risk stratification expired in September 2023. [↑](#footnote-ref-26)
38. It is worth noting that the approval NHSE received for processing personal data for risk stratification expired in September 2023. [↑](#endnote-ref-14)
39. Eclipse stands for Electronic Checking Leading to Improved Prescribing Safety & Efficiency and appears to be owned by Prescribing Services Ltd. [↑](#footnote-ref-27)
40. <https://www.snowflake.com/en/> [↑](#endnote-ref-15)
41. <https://aws.amazon.com/financial-services/partner-solutions/snowflake/> [↑](#endnote-ref-16)
42. <https://aws.amazon.com/financial-services/partner-solutions/snowflake/> [↑](#endnote-ref-17)