CASE STUDY OF THE SOUTH EAST LONDON INTEGRATED CARE SYSTEM (ICS): AN EXAMPLE OF HOW ICSs ARE USING PATIENT DATA

Keep Our NHS Public Health Data Working Group
(in collaboration with South East London Save Our NHS)
May 2023

Summary

The collection, analysis and sharing of patients' data has become essential for the work of Integrated Care Systems (ICS): this data informs direct patient care, the commissioning and planning of services (including cuts), Population Health Management and workforce planning, Patients' data is also, potentially, a highly valuable resource for some of an ICS's 'partners' and sub-contractors, whether for research or commercial exploitation.

Current legislation provides little protection for our personal data if its use is 'in the public interest' and existing protections are under threat. It has never been more important for health campaigners/data subjects to be informed and able to challenge what is happening to patient data.

With this in mind, the KONP Data Working Group, in collaboration with South East London Save Our NHS, looked into the way that one ICS (South East London), collected and used patients' data. Our main aims were to understand how best to monitor and, if necessary, challenge the way personal data is being used, and to provide information and suggested questions for other health campaign groups that want to to do this as well.

The main issues we found concerned a lack of clarity about data governance arrangements and poor lay representation; the use of data without consent; risks to confidentiality; lack of patient and citizen engagement and the fast growing role of the private sector, with no clarity about the access that companies have to individuals' records.

The report includes two appendices providing template questions to put to local ICBs and suggestions for how to make the best use of these questions.

To conclude, forthcoming legislation favouring the interests of Business is only likely to weaken safeguards for our NHS data. For now, at least, it seems that the most effective way of countering the increased access to our data is to understand what is happening, insist on the protections that we still have, and demand accountability and transparency on the part of those using our data: if those responsible for the use of our health data are aware that the public is monitoring them, it may at least help to ensure that they carefully consider their actions.

INTRODUCTION

The collection, analysis and sharing of patients' data has become essential for the work of Integrated Care Systems (ICS): the data informs direct patient care, the commissioning and planning of services, workforce planning, the use of risk stratification and Population Health Management (PHM), the identification of 'unnecessary variations' in health and healthcare while it facilitates a shift towards 'patient level costings' and 'sustainable healthcare' (cuts in NHS services). Patients' data is also, potentially, a highly valuable resource for some of an ICS's 'partners' and sub-contractors, whether for research or commercial exploitation.

The extraction of data from patients' personal records often sits uncomfortably with existing legal protections. UK data protection legislation[1] and the data watchdog, the Information Commissioner's Office (ICO), currently govern the use of data from patients' medical records. However, in many instances it is possible for organisations such as those within an ICS to work around data protections, although the legitimacy of this is not always clear. On top of which, the government is planning to weaken existing safeguards, favouring instead the interests of Business, having already muzzled the ICO. This raises questions about how confident anyone can be about the safety of patient data in the current context and beyond.

With this in mind, the KONP Data Working Group, together with South East London Save Our NHS (SELSON) has looked into the use of data by the South East London ICS (SEL ICS), a pioneer in the use of patient data services. Our aims have been

- to learn how NHS patients' data is being used at the local level, with a view to identifying how this use can be monitored and, when appropriate, challenged,
- to provide an example of what is happening in one ICS that may be useful for campaigners elsewhere who are interested in finding out how their local ICS uses patients' data, and
- to develop a number of questions about data use that can be adapted as necessary to local circumstances for interested campaigners to put to their ICB or submit as Freedom of Information (FOI) requests, either for clarification purposes or to challenge existing practice.

Information about the SEL ICS and its use of data was gleaned from a variety of sources, such as the ICS's Integrated Care Board (ICB) papers, its Governance Handbook, the ICS's website, and Freedom of Information (FOI) requests, as well as by word of mouth and questions put to the ICB.

For clarity, we use the term 'ICB' to refer to the IC Board, its various committees and decision-making groups, while 'ICS' is used to refer to the wider system made up of partner organisations. This report mainly focuses on the ICB.

The research was carried out in late 2022/early 2023, during the early days of the ICS when its structure and processes for data management were still under development. The report therefore provides a transitory picture. Nonetheless, it is hoped that it will still provide a useful snapshot.

Findings from the research are organised into five themes (governance, use of patients' data, legal issues, patient and citizen engagement, and private company involvement).

[1] Such as the UK General Data Protection Regulation (GDPR) and the Data Protection Act (DPA 2018)

The questions we developed in response to our findings can be found in Appendix Two. For suggestions about the use of these questions, see Appendix One.

THEME 1. GOVERNANCE

Despite data being crucial to the operation of the ICS, we found that, in the case of the SEL ICS, their formal published material was unclear about where many decisions about data are made and how the use of data is governed across the ICS: for example, charts of the organisation's structure.

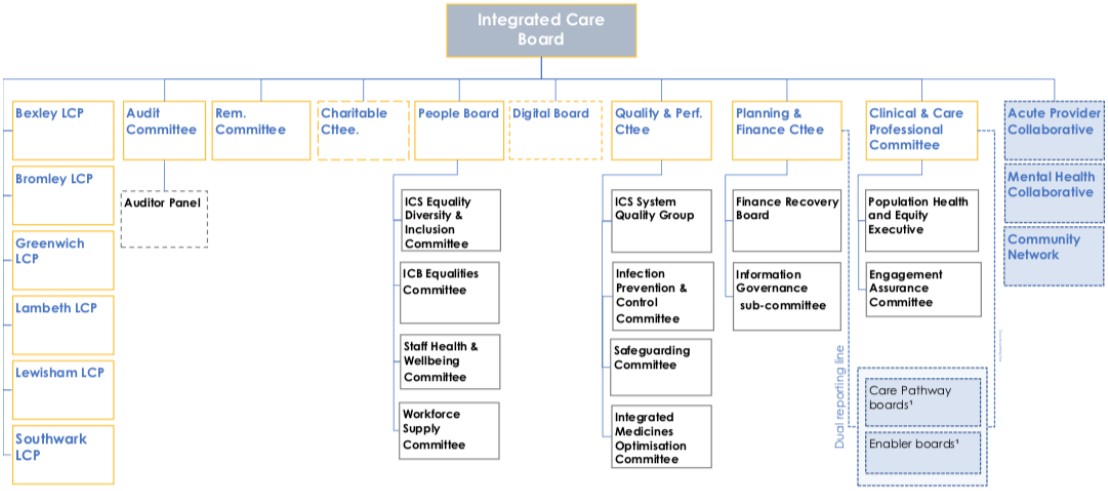

Fig 1. (as of April 2023)

Ultimately, the ICB is accountable in law for the data that the ICB handles and processes. Currently all personal data that the ICB processes falls within the remit of the DPA (2018) and the UK GDPR. That said, organisations within the ICS (such as NHS Trusts) will each have their own data controller responsibilities and – as established by the UK GDPR - neither the ICB nor the other partner organisations within the ICS can overrule these.[2]

In SEL, co-ordinated responsibility for information governance sits within the ICB's Operations Directorate, and responsibility for the use of data for business intelligence and analytics sits within the Planning Directorate. At the same time, acute providers and local authorities will also have their own systems for information governance.

More precisely, we found that the ICB structure includes:

- **A Digital Board**

This is responsible for the development of the ICB Digital Strategy; developing investment cases and funding bids for system wide digital schemes and investment; and aligning digital solutions and systems across SEL. The Digital Board reports directly to the ICB. In response to a question from SELSON, we were told meetings of the Digital Board are not open to the public and there is no intention at the moment to publish its papers.

- **An Information Governance Sub-committee (IGSC)**

[2] In response to a question to the North East London ICB, this means that any processing by an ICB or ICS must be agreed by all relevant data controllers following a Data Protection Impact Assessment (DPIA).

This oversees the management of the ICB's Information Governance Framework, work plans, security and risks. Its remit includes confidentiality and consent, data protection, information sharing (including transfers abroad), oversight of the wider Information Governance Group (undefined), IG training and records management. It reports to the Planning and Finance Committee. The IGSC is the body that ensures that the ICB complies with legislation and other IG requirements (such as those of the Department of Health and Social Care). The Sub-Committee membership includes a Caldicott Guardian[3] and two deputies, and a corporate representative,[4] but no lay representative.

- **A Digital Transformation Board**

(Referred to in SEL ICS's documents but details are currently unknown.)

- **A Data Usage Committee (DUC)**

The DUC is key in approving applications to access and use patients' data for non-direct care and has responsibility for records management, data quality and disaster recovery. It is also the body charged with overseeing the Discovery Data Service (see below) on behalf of the SEL partners.[5] However, unlike the now defunct NHS Digital Independent Group Advising on the Release of Data (IGARD),[6] the DUC does not appear to publish its minutes, and its List of Approved Data Requests[7] provides only skeletal information about its activities. It seems there has been some difficulty in approving the Committee's Terms of Reference and it remains unclear to whom it is accountable.

- **A Business Intelligence Unit (BIU)**

The Business Intelligence function covers statutory reporting, strategic planning, care delivery, performance management, population health management and research, both at the level of the separate organisations within the ICS as well as at ICS system-level. Currently, each organisation has its own team of analysts looking through their own particular 'lens'. (A review is due to consider the preferred model for analytical services). The BIU is part of the Planning Directorate and accountable to the Director of Planning.

- **A Population Health Management and Inequalities Board (PHMIB)**

The PHMIB works across the ICS to improve intelligence and analytics, for example, in order to create a coherent longitudinal record of a person's health and care; bring in other sources of data to generate a resource for planning and decision-making at patient level; carry out segmentation and stratification of the ICS population and commission/deliver services that address the needs identified while providing evidence to justify interventions. The Board appears to report to the Clinical and Care Professional Committee.

- **A Population Health Equity Executive (PHEE)**

---

[3] A Caldicott Guardian has a senior position within an organisation that processes health and social care personal data. They ensure that the personal information about those who use the organisation's services is used legally, ethically and appropriately, and that confidentiality is maintained. Their primary concern is information relating to individuals and their care, but the need for confidentiality extends to other individuals, including their relatives, staff and others.

[4] Details of who this corporate representative is, or which organisation they represent are not clear.

[5] https://www.selondonics.org/wp-content/uploads/SEL-ICB-Privacy-Notice-Data-Service-v2.0.pdf

[6] IGARD provided oversight of NHS Digital's processes to ensure they were appropriate for governing the receipt, processing and publication of data; ensured confidentiality; and independently assessed applications for data.

[7] https://www.selondonics.org/wp-content/uploads/2022/11/SEL-ICS-WEBSITE-Approved-DUC-Applications-Nov-2022.pdf

The PHEE is a sub-committee responsible for embedding a population health approach across all of the ICS's activities. It oversees a joint programme of work between the SEL ICS and Kings' Health Partners, which includes Population Health Management (see below) and data. The sub-committee reports to the IC Board and IC Partnership and is supported by a Population Health Equity Partnership Advisory Group, with membership from across health, social care, public health and wider within the ICS and contributes to strategic and operational input. The Executive can also identify 'potential partners' with whom to collaborate on specific workstreams aligned to the ICS's Population Health Equity Programme and establish an 'Anchor' system that recognises the assets of staff, population, organisations and communities. Membership of the PHEE does not seem to include representatives from any of the data committees or sub-committees mentioned above.

In sum, there are a range of different bodies within the SEL ICB that influence the use of data, each looking at this through a different prism. There is little to no publicly available information about their activities or about public representation.

THEME 2: USE OF PATIENTS' DATA

NHS England (NHSE) has stipulated that each ICS must

> "develop or join a shared care record joining data safely across all health and social care settings, both to improve direct care for individual patients and service users, and to underpin population health and effective system management"[8]

In line with this, SEL ICS is moving to towards a single view of a person's health and care record, developed from shared records, that can inform patient care, wherever they present. This single view initially took the form of the London Care Record.

The London Care Record

Recent years saw the introduction of the Local Care Record giving acute users access to GP information. Now, however, the Local Care Record is being replaced by the London Care Record, under the auspices of One London.

One London[9] is a collaborative of London's five ICSs and the London Ambulance Service (and one of a number of collaboratives being formed across England). It is supported by NHSE (London Region), the Greater London Authority and London's three Academic Health Science Networks while, critically, governance sits within NHSE London.

Each of London's ICSs (plus Hertfordshire and West Essex and Milton Keynes ICSs) have their own systems for sharing data within their areas.[10] The London Care Record collects the information in these systems and creates a combined view of an individual's patient's records that is available to health care professionals (such as doctors, nurses and social workers) across London and the surrounding area.

---

8. https://www.england.nhs.uk/wp-content/uploads/2021/01/integrating-care-next-steps-to-building-strong-and-effective-integrated-care-systems.pdf

9 https://www.onelondon.online/about/

10 https://www.onelondon.online/london-care-record-organisations/

Data for the London Care Record is extracted from a variety of sources (such as primary and community care, out of hours care, A&E care, and hospital care) by a number of (commercial) service suppliers.[11] The data includes a patient's full address, date of birth, NHS number, conditions, medications, allergies, appointments, clinical encounters, observations, diagnostic reports, plus warnings and flags. For those with the right password, access to an individual's Summary Care Record[12] (which can be useful in emergency situations) requires just one of the following: name, date of birth, Patient ID or NHS number.

The London Care Record is supported by a central Health Information Exchange (HIE) provided by Oracle Cerner. This central hub connects to a series of local HIEs, providing a single record of a patient's health and social care information.

According to the SEL ICB in a response to a question posed by a member of the public, the London Care Record is only accessed for direct patient care. However, it transpires that patients' personal data collected from GP practices[13] and other healthcare providers is accessed both for direct care *and* for other purposes (such as service planning and population health management) via the Discovery Data Service.

The Discovery Data Service

The South East London ICB is one of three involved in developing the Discovery Data Service (DDS), which is now interoperable across all London ICSs. Although the service is only relevant to London at the moment, we report on it in detail in case it helps to flag up issues about the data services that ICBs are using elsewhere.

The DDS is a cloud-based, live data service capable of handling health and care data from across the UK's whole population. Essentially, data is submitted from organisations providing primary, secondary, and urgent care services to patients or clients.[14] Once transformed into a common model, the data store can be used at an individual level (for example, by an NHS 111 call handler responding to a patient) or at a population level (for instance to identify a group of people with asthma where algorithmic profiling suggests that they could benefit from a proactive intervention, although the validity of this approach has been questioned.)[15]

To clarify, the 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,

---

[11] https://wiki.discoverydataservice.org/index.php?title=Current_data_sets

[12] The Summary Care Record (SRC) contains basic information about an individual's allergies, medications and any reactions to medications in the past. Some patients, including many with long term health conditions, have previously agreed to have Additional Information shared as part of their SRC.

[13] All healthcare organisations, including GP practices, that provide direct care should have a Senior Information Risk Owner, a Caldicott Guardian and a Data Protection Officer in place but each organisation will probably manage data governance arrangements differently.

[14] The data sets that are currently received by the DDS from different supplier systems can be seen here: https://wiki.discoverydataservice.org/index.php?title=Current_data_sets

[15] Algorithmic profiling (AP) has been described as "a method of inferential analysis that identifies correlations or patterns within datasets that can be used as an indicator to classify a data subject as a member of a group". It has been suggested that the fundamental aim of AP is to discriminate, that it targets marginalised groups and perpetuates hierarchies based on implicit assumptions built into the development of algorithms. https://journals.sagepub.com/doi/full/10.1177/2053951719895805

quality and care improvement, health and care commissioning, population health management and "cross care-setting innovation"[16] (presumably meaning integrated service re-design), subject to data sharing agreements, consent and satisfactory security arrangements.

For example, the DDS provides outputs in different formats to the SEL's ICS's Business Intelligence Unit and the ICS Clinical Effectiveness and Population Health Management programmes, as well as researchers and epidemiologists through, for instance,

- *Discovery Explorer,* a web-based application dealing with queries to provide extracts, dashboards or reports on request, including cohort identification for intervention studies needing personal data, anonymous data for research and personal data for direct patient care, and
- *Discovery Compass,* a copy of the DDS data designed to meet specific requirements, such as anonymous data for epidemiology; pseudonymised data for linkage to external data sets; and personal data, anonymised and pseudonymised data for Population Health Management (PHM)[17]

The DDS is owned by the NHS with governance arrangements described as 'bottom up': those party to a data sharing agreement decide on their specific governance model.[18] We were unable to discover the governance arrangements for the DDS itself.

Data privacy

While the disclosure of completely anonymised or aggregated data sets by GPs, hospital trusts or other data controllers (e.g. for inclusion in the DDS) is lawful for purposes beyond direct care, this is only *as long as anonymisation takes place at source*.[19] This does not seem to be the case with data transferred to DDS. As previously noted, in addition to hosting the London Care Record, the DDS has the separate function of processing confidential information extracted from GP records, NHS hospital and community Trusts and Local Authorities (social care data) and disclosing this to third parties for secondary uses, either as aggregated, anonymised, pseudonymised or clearly identifiable data sets.[20] [21]

Significantly, what can be defined as anonymous data is changing. Until now, anonymisation meant that information that identifies a patient has been removed. Currently, patients' data is not considered to be confidential if the process of

---

[16] Description taken in part from the *One London* Local Health and Care Record Exemplar business case.

[17] Information on Discovery Explorer and Compass originally from https://wiki.discoverydataservice.org/index.php?title=Welcome_to_the_London_Discovery_Data_Service_knowledge_base but now removed.

[18] According to a response from NHS London Shared Service to a FOI request about the DDS and information governance, "use of the DDS is governed by the Terms of Reference (ToR) which apply to each participating organisation. Those ToR address data protection compliance by reference to the functionality of the DDS, including the workings of the Data Access Group." (June 2022) (https://www.whatdotheyknow.com/request/853629/response/2058557/attach/3/FOI.22.NEL010%20Response.pdf?cookie_passthrough=1)

[19] https://www.nhsdatasharing.info

[20] https://www.nhsdatasharing.info/CLoC/DDSdataflow.pdf

[21] We are unclear about how the work of a data service like DDS relates to that of Data Services for Commissioner's Regional Offices (DSCRO), which at least in the past, had the legal responsibility for de-identifying personal data before it was passed to Commissioning Support Units. https://digital.nhs.uk/services/data-services-for-commissioners/data-services-for-commissioners-regional-offices#about-data-services-for-commissioners-regional-offices

anonymisation meets the requirements of the ICO's anonymisation code of practice.[22] This code is currently under review but proposals include that data can be 'effectively' rather than 'truly' anonymised if, for example, the means required to re-identify an individual from the data are considered 'prohibitive'.[23] The Data Protection and Digital Information Bill also proposes to give data controllers discretion to decide when personal data can be classified as anonymous. Notably, data protection law does not apply to anonymised data.

Recently, the National Data Guardian and UK Caldicott Guardian Chair of Council (NDG & CCC) jointly expressed concern that, within some data sharing programmes, organisations are using confidential patient information (CPI) without ensuring that their activities did not breach confidentiality.[24] They emphasise, for example, that sharing data from local record sharing programmes with Secure Data Environments (like the DDS) for purposes other than individual care cannot rely on patients' implied consent. They also point out that organisations wishing to set aside the common law duty of confidentiality[25] should consult the Confidential Advisory Group (CAG)[26] on whether they can lift the duty of confidentiality (see Theme 3 below for more details).

Population Health Management (PHM) and risk stratification

a) Population Health Management

PHM, an approach that comes from the USA that is premised on value-based care,[27] has been described as

> "the process of improving clinical health outcomes of a defined group of individuals through improved care coordination and patient engagement, supported by appropriate financial and care models." [28]

It allows organisations to identify physical and social determinants of health with a view to pre-empting illness.

The population of interest can be small or large and defined, for example, by geography, diagnosis or other features (such as a common insurance provider in the USA). The process begins by gathering key clinical and other data from patients' electronic health records, before sorting patients into categories based on clinical history and risk. Analysts then use aggregated data (for example on types of chronic disease, residence in a low-income community or frequent hospitalisation) for risk stratification.

---

[22] https://digital.nhs.uk/services/national-data-opt-out/understanding-the-national-data-opt-out/confidential-patient-information

[23] https://ico.org.uk/media/about-the-ico/documents/4018606/chapter-2-anonymisation-draft.pdf

[24] 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

[25] In common law, there is a duty of confidentiality which means that when a patient/service user shares information in confidence it must not be disclosed without some form of legal authority or justification. In practice, this usually means that the information cannot be disclosed without that person's consent.

[26] The CAG is an independent body providing expert advice on the use of confidential patient information. This includes advice to the Health Research Authority for research uses, and the Secretary of State for Health and Social Care for non-research uses. It aims to protect the interests of patients and the public while enabling the appropriate use of confidential patient information for purposes other than direct patient care.

[27] A value-based approach is concerned with improving a patient's health outcomes relative to the cost of care. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7185050/ For more information, see "The (mis)use of 'value' in Integrated Care Systems (ICSs) to enable financial cuts", https://keepournhspublic.com/integrated-care-systems/

[28] https://healthitanalytics.com/features/howpopulation-health-risk-stratificationsupportvalue-based-care

As the multinational corporation Deloitte makes clear, PHM 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. PHM also provides a way of identifying 'unwarranted variation' in health and care,[29] which can provide the means for rationing treatments.[30]

As mentioned, PHM is reliant on aggregating a range of data sets. One implication is that, even if personal data is pseudonymised,[31] the more that data is linked at an individual level, the greater the probability there is of identifying individuals. This raises the question of how closely are those using patients' personal data complying with data protection legislation.

b) Risk stratification

PHM is strongly associated with risk stratification, "an ongoing process of assigning all patients a particular risk status" based on data that flags up health indicators, lifestyle, and medical history. [32] It involves processing secondary and primary care information to either

a) identify vulnerable or at risk *individuals* who might benefit from some form of intervention that aims to reduce the likelihood of health deterioration or crisis, or
b) identify *groups* of individuals facing similar health inequalities who might benefit from some kind of intervention.

Notably, suppliers of risk stratification processing will usually process personal confidential data in either a pseudonymised or de-identified form (i.e. with an individual's NHS number as the patient identifier removed), with processing taking place within a 'closed box'. Re-identification then allows individual patients to be identified by those providing direct care (such as a GP), in order to consider suitable interventions.[33]

An ICB must make arrangements to ensure that the public understand the proposed use of data for risk stratification purposes between a commissioner and provider of NHS funded health services (including an explanation of risk stratification, information about who the data controllers and processors are, what type of data will be used, and the individual's rights, e.g. to access the data or to object). The SEL ICB has produced a rather confusing Privacy Notice about risk stratification[34] that implies patients will be informed by their GP surgery about this use of their data, but it is unclear when or how patients are provided with this information. Significantly, the Privacy Notice states that

---

[29] https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/public-sector/deloitte-uk-public-sector-population-health-management.pdf

[30] https://doctorsinunite.com/2020/03/02/rationing-in-the-nhs/

[31] Pseudonymisation replaces 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.

[32] https://healthitanalytics.com/features/howpopulation-health-risk-stratificationsupportvalue-based-care

[33] https://www.westyorkshire.icb.nhs.uk/privacy-notice/risk-stratification

[34] The ICS Data Service Privacy Notice, for example, provides information on the purposes of DDS, and about the three key sub-processors, and refers to the DUC and its Terms of Reference (link not functioning), how to opt out, and the legal basis the ICS relies on for risk stratification. Yet it gives no information about how to contact data controllers or the data used and gives no explanation of risk stratification.

"You have the right to object to our sharing your data in these circumstances, but we have an overriding responsibility to comply with our legal obligations".

THEME THREE: THE LEGAL BASIS FOR THE USE OF PATIENTS' DATA

The lawful basis for processing patients' data depends on why the data is being processed. Generally, processing falls under one of the statutory obligations of an ICB. These include the duty to improve the quality of services and the duty to reduce inequalities (under the Health and Social Care Act 2012 (HSCA 2012, s26) and the NHS Act 2006, s14T); the duty to exercise the ICB's functions effectively, efficiently and economically (HSCA 2012, s26); and the duty to secure continuous improvement in the quality of primary medical services (HSCA 2012. s26).

In addition, the *protection* of patients' data is largely dependent on the following:

a) The Common Law Duty of Confidentiality

In practice, it is assumed that a patient or service user receiving treatment or care has implicitly agreed to their relevant confidential information being shared with others involved in their care ('implied consent for individual care'). Legally, this confidential data is protected by the Common Law Duty of Confidentiality (CLDC), which prevents such information from being disclosed without some form of legal authority or justification. The CLDC also requires that a duty of confidentiality is established within professional codes of conduct and/or must be included within relevant employment contracts. The CLDC extends to confidential information that is received from other organisations where the data subject would reasonably expect that any recipient would hold it in confidence.[35]

However - in contrast to the sharing of data for direct patient care - the secondary use of GP and Secondary Uses Services (SUS)[36] data for *processing* purposes cannot be based 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 "section 251 support" of the NHS Act (2006) (known as 'CAG 7-04 (a)/2013' – see below for more detail).[37]

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 the 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. This approval is known as CAG 7-04(a)/2013. In 2022, in order to cover the transfer of CCGs' responsibilities to ICBs, the approval was extended to allow the use of GPs' and ICBs'

---

[35] https://transform.england.nhs.uk/media/documents/NHSX_IG_Framework_V6.pdf

[36] Secondary Uses Services (SUS) is a repository for information collected from patients' use of secondary care services such as in-patient, out-patient, A&E and the mental health services that, in addition to supporting a patient's treatment also made available to commissioners and providers of NHS funded care for purposes such as healthcare planning and development of national policy.

[37] 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.

secondary data for risk stratification purposes until the end of September 2023. (The approval does not cover disclosure of social care data for risk stratification.)

However, such 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[38] 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.[39] 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.

In a recent letter to ICBs, the National Data Guardian and UK Caldicott Guardian Chair of Council (NDG & CGCC) highlight their concern that, in combining CPI for risk stratification, some organisations rely on implied consent as a legal basis, instead of making a process-specific application to the CAG.[40] In addition, they note that some organisations use risk stratification processing not just to select and target vulnerable populations but, rather, to inform wider population health management programmes. Here data mining is more extensive than the limited data extraction covered by CAG 7-04(a) 2013 (e.g. it additionally involves the disclosure of social care data),[41] while some of those involved in the processing may not be on the list of organisations approved to do this.

A further concern expressed by the NDG & CGCC is that, where ICBs plan to use patient data to support the effective functioning of the ICS, they should, if possible, do this with information that has been rendered anonymous. However, transferring CPI to a third party that is not collecting it for direct care but to anonymise it prior to secondary processing cannot rely on 'implied consent' as an appropriate legal basis. In such a scenario, the ICB should consider applying for support under Section 251 of the NHS Act 2006, while also ensuring that all anonymisation processes used are in line with ICO guidance.[42]

---

[38] 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/

[39] https://www.england.nhs.uk/publication/risk-stratification-assurance-statement/

[40] 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.

[41] Where social care data are to be used then the relevant parties need to assure themselves there is a legal basis for the disclosure and linkage for this purpose, and then either use a third party and pseudonymised data or consent.

[42] https://ico.org.uk/about-the-ico/ico- and-stakeholder-consultations/ico-call-for-views- anonymisation-pseudonymisation-and-privacy-enhancing- technologies-guidance/

The NDG & CGCC also note that there must be due regard for public trust, especially where commercial arrangements existed between care providers, third party processors and researchers.

b) The UK GDPR

To complicate matters, the UK General Data Protection Regulation (GDPR) has a higher threshold for consent than the CLDC: for example, it does not recognise the concept of implied consent. Instead,

> "consent should be given by a clear, affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data".[43]

There is also a mandatory obligation under UK GDPR for organisations that provide services and share data on the basis of 'informed consent' to inform patients and service users about how their information may be used *before it's shared*, for example through 'transparency materials' (previously referred to as 'privacy notices').

However, the UK GDPR provides a number of legal bases, besides consent, allowing publicly funded or statutory health and social care organisations to undertake lawful processing. To process special category data (which includes information about an individual's health, their genetic data and racial or ethnic origin), the processor must identify a lawful basis under Article 6 of the UK GDPR *and* a separate condition for processing under Article 9.

Article 6 provides six lawful bases for processing personal data, including Article 6.1 (e) – probably the most relevant to ICBs. This applies when "processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller". Significantly, the ICO describes this condition as 'public task' and clarifies that the task or function concerned should have a clear basis in law.[44]

Article 9 states that processing special category data is prohibited unless certain conditions apply. These include if explicit consent has been given and if there are 'reasons of public interest'.

The UK GDPR and 'right to know' and object

A key transparency requirement under the UK GDPR[45] gives individuals the right to be informed about the collection and use of their personal data. This 'privacy information' (which must be provided to individuals *when the data is collected*) includes the purposes for processing, how long data is retained for and with whom it will be shared. There are though some circumstances where it is deemed unnecessary to provide privacy information (such as if it would involve "a disproportionate effort to provide it").

Article 21 of the UK GDPR gives individuals the right to object to the processing of their personal data, and also makes it clear that individuals must be informed of this right. However, the right only applies in certain circumstances, depending on the purposes for processing and the lawful basis claimed for processing.

---

[43] https://transform.england.nhs.uk/information-governance/guidance/consent-and-confidential-patient-information/#ig_professional

[44] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/#how

[45] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/

c) The Data Protection Act (DPA) 2018 and 'substantial public interest'

The DPA sets out 23 conditions that provide a legal basis for processing special category data for reasons of 'substantial public interest'.[46] The term 'public interest' covers a wide range of principles and values relating to what is in the best interests of society. Those wishing to process special category data on the basis of substantial public interest must identify the most relevant condition and provide specific arguments, such as the amount of benefit expected from the processing, or the volume of people who would benefit. The most relevant condition out of the 23 given appears to be 'protecting the public'.

An ICB might suggest, if questioned, that it processes special category data to identify and address inequalities in health and target resources to those most in need and thus in the public interest. If so, this might prompt further questions about whether there is robust evidence to demonstrate that PHM and its use of special category data is effective in addressing inequalities or whether PHM is primarily concerned with rationing services and therefore is not at all in the public interest.

Data use, confidentiality and the SEL context

Prompted by the concerns of the NDG & CGCC, SELSON put a question to the SEL ICB Board meeting of November 2022, asking for a list of organisations and companies (including those accredited through the Health Services Support Framework) that collect and provide patient data for research and planning purposes in addition to direct patient care.

The response made no mention of any companies involved in collecting or providing patient data. It stated that data from the Local Care Record and London Care Record are only used in delivering direct patient care: third parties, such as companies (including those on the HSSF) or individuals not directly involved in a patient's care cannot view or access their data.

However, in describing the data services it is developing to support PHM, care and service planning,[47] the SEL ICB states that it is bringing together important health and care information into a single space, 'organising' it and then making it available to appropriate health care professionals and service leaders: "This will support decision making relating to individuals' direct care, service design, transformation, overall population health and important research." In other words, patients' data is available to those who are not directly involved in their care.

Notably, alongside recognising the rights of individuals under the CLDC, the SEL ICS's Privacy Notice on data use indicates that it relies on Article 6(1)(e)[48] of the GDPR for "[t]he processing of personal data for the delivery of Risk Stratification and for providers' administrative purposes",[49] on the basis that disclosure is in the public interest. It makes no argument for why it is in the public interest to lift the duty of confidentiality.

---

[46] Paragraphs 6 to 28 of Schedule 1 of the DPA 2018.

[47] https://www.selondonics.org/who-we-are/our-work/digital-and-data/data-services/

[48] Article 6(1)(e) i.e.'...necessary for the performance of a task carried out in the public interest or in the exercise of official authority...'.

[49] https://www.selondonics.org/wp-content/uploads/SEL-ICB-Privacy-Notice-Data-Service-v2.0.pdf

The SEL ICB Privacy Notice on data also mentions Article 9(2)(h) of the GDPR. This refers to the processing of special category data,[50] which states that processing personal data is not prohibited when it is

> "necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of domestic law."

However, according to Article 9.3, the processing of special category data referred to in point (h) is conditional: data should be processed by, or under the responsibility of, a professional or other person (as defined in Section 204 of the DPA 2018) who is subject under domestic law to the obligations of professional secrecy. Although the Data Protection and Digital Information Bill may change things in future, at the moment, data analysts are not included in the recognised list of professionals who owe an obligation of confidentiality.

THEME FOUR: PATIENT AND CITIZEN ENGAGEMENT

The SEL ICS makes various references to patient or citizen engagement – e.g. the SEL Digital Strategy states that the ICS's primary objective is "to deliver person centred care informed by systematic patient engagement and involvement of the service user". There is also mention that the ICS ran a communications and engagement campaign during 2021.

However, an FOI request submitted by SELSON asking how the public is represented in digital matters, or how it can get involved, received the following limited reply:

> "NHS South East London ICB does not hold this information. The smaller digital and data programmes have traditionally had patient representation through SEL Healthwatch. You may wish to contact the Director of South East London Healthwatch for further information at https://healthwatchgreenwich.co.uk/."

The Digital Strategy refers to the importance of liaising with SE London Healthwatch, whose Director is a member of the SEL Information Governance Group, to ensure the trust and confidence of local people. It is unclear though if Healthwatch is always a member of decision-making bodies. (We know by word of mouth that it has two members on the Data Usage Committee).

A question to the Board from a member of the public also raised concern that people across SE London had not been consulted or told that the ICB was using Discovery to collect and share data for research and planning, even though it had been importing 10 years of detailed primary care data and, more recently, secondary care data including data on mental health, community and social care.

The response was that the ICS had been raising awareness about the London Care Record through short films and stills, posters and information leaflets in organisations that participated in the London Care Record programme. In addition, engagement work

[50] Special category data is personal data that is sensitive: its use could expose significant risk to an individual's rights and freedoms and so it needs additional protection. The special categories of personal data concern racial or ethnic origin, political opinions, religious or philosophical beliefs, trades union membership, genetic data, biometric data (when used for identification), health, sex life and sexual orientation.

had been carried out via the One London programme, such as a citizens' engagement project and summit in early 2020[51] and further work in 2022.[52] (Reports from these projects have been criticised for cherry picking the views of participants to suggest unconditional approval for data sharing.)

The ICS's response also said that,

> "The use and access to data, via the *Discovery Data Service*, is underpinned by data sharing agreements, which give details of particular projects as well as the specific policies in respect of people's rights and consent. Some projects will require specific consent and others will be aligned to the national opt-out process. More detail is available on the discoverydataservice.org website."[53]

However, the detail referred to is not aimed at the general public.

An additional question from SELSON asked how members of the public will be informed about how to Opt Out if they do not want their health or their social care data used in this way. The response included a link for individuals to opt out of their data being submitted to the local Opt-Out, and mention of the National Data Opt-Out for those who do not wish their data to be used for secondary purposes - but no indication of how to register for this. However it clarified that if an objection was registered,

- "For Discovery Data Services, this is managed by us or by the NHS NEL ICB team who host the service, or the SEL ICB for internal projects.
- It is NOT applicable to the London Care Record as this system is ONLY used for Direct Care purposes.
  All south east London organisations are required to comply with the opt-out process, and ensure that information about the opt out is on their website.[54]

THEME FIVE: PRIVATE COMPANY INVOLVEMENT

Looking at the use of patients' data by SEL ICS, what becomes clear is how the reliance on data and data services has further opened the NHS to private (generally multinational) companies: the private sector, often in the shape of US based corporations, is now deeply embedded in the NHS at local level.

Take electronic health records, for example. In SEL, primary care services data will converge on the *EMIS Web* platform (now owned by Optum, part of UnitedHealth),[55]

---

[51] https://onelondon.online/citizenssummit/

[52] https://www.onelondon.online/wp-content/uploads/2022/10/A-deliberation-on-Londons-health-and-care-data_FINAL.pdf

[53] A glance at information on case studies indicates that some projects applying for access to DDS data have access to patient identifiable data. E.G. the Whole Systems Data Project (applicant Tower Hamlets CCG) requires patient identifiable and anonymised data to "Establish an integrated health, social care and wider determinants of health dataset across Tower Hamlets that allows effective risk stratification and needs-based resource allocation for the local population based on evidence."
https://wiki.discoverydataservice.org/index.php?title=Whole_Systems_Data_Project

[54] For opting out of social care data collection see https://www.digitalsocialcare.co.uk/data-security-protecting-my-information/national-data-opt-out/.

[55] EMIS has been the dominant EHR 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.

while acute Trusts are using *Oracle Cerner Millennium* and the *Epic* EHR. Mental health services are working with King's Health Partners and UCLH hospitals to develop *Cogstack*[56] and natural language processing to scan records for free text that flags up potential crises. Community services currently use a range of Electronic Health Records, including *UnitedHealth/EMIS, Rio* and *Epic.* Pathology services use the *Synnovis* partnership (with 51% of shares in the hands of Labco UK Group, owned by Synlab International, registered in Germany), while in social care, care homes have access to *Coordinate My Care* (now being incorporated into the London Care Record). The London Care Record uses the *Oracle Cerner HIE platform t*o drive the shared care record, with access for primary care staff provided via a *UnitedHealth/Emis* portal.

Turning to the Discovery Data Service, the data sets they currently publish are sourced from *UnitedHealth/EMIS, SystmOne* (Part of the *Phoenix Partnership TPP*), *INPS Vision* (part of *Cegedim*, a global technology and services company), *Adastra* (a global company providing data services),[57] *Oracle Cerner Millennium* (part of *Oracle*, a US based technology company), *Silverlink* (part of *Alcidion*, a company founded in Australia) and *Medway.*[58]

However, perhaps an even greater opportunity for the private sector comes from 'integrated care', risk stratification and PHM. For example, contracts for supplying risk stratification services to ICBs can only be awarded to certain companies, namely *Bupa HD*, *Capita, Oracle Cerner, Docobo, Health Intelligence, Dr Foster Intelligence, MedeAnalytics, PI Benchmark (Care and Health Trak), Sollis, United Health (Optum), Nottingham Health Informatics Service, Prescribing Services Ltd, EMIS, TTP SystmOne, MSD Ltd, Graphnet.*[59]

The SEL ICS's Population Health Management programme has been supported by NHSE in partnership with *NECS* and *Optum* (part of US based *UnitedHealth Group*), apparently to build capacity. To date, the focus for PHM nationally has been to put in place ETL[60] and shared care record solutions. However, once in place the focus will shift to using the data pool that these have created to drive PHM. The ICSs, PCNs, acute trusts and other primary/community NHS providers will all be looking at ways in which this new pool of harmonised patient data can be best exploited. We can only expect to see more contracts, supported by NHS funding streams, such as the Unified Tech Fund, for PHM analytics and care management platforms.

It's becoming increasingly clear that a significant number of the multinationals profiting from providing data and digital services to the NHS have tarnished records in terms of probity. For example, EMIS and Optum are both owned by UnitedHealth, which since

---

[56] Cogstack is an open source, application framework that allows the extraction of information from unstructured data sources (such as EHRs) in multiple formats (e.g. PDFs, text fields, images). Once extracted, harmonised and processed, multiple uses of this unstructured data become possible, including Natural Language Processing. Cogstack has also been seen as a tool to provide "a more efficient way to clinically code to improve financial and operational efficiency". *https://transform.england.nhs.uk/ai-lab/explore-all-resources/understand-ai/cogstack/*

[57] The founder of Adastra is a trustee of The Endeavour Health Charitable Trust that funds the DDS.

[58] Details of the data sets published by these companies to the DDS, and their source (e.g. GP primary care, out of hours services, A &E), can be seen here: https://wiki.discoverydataservice.org/index.php?title=Current_data_sets

[59] https://www.england.nhs.uk/publication/risk-stratification-assurance-statement/

[60] ETL (Extract, Transform and Load) is a data integration process that combines data from multiple data sources into a single, consistent data store that is loaded into a data store.

2000 has been fined $469,099,518 for 'customer protection-related offences', and $131,539,180 for 'government contracting-related offences'.[61]

CONCLUSION

Research into SEL ICB's use of data is still on-going but initial findings suggest that private companies, whether providing technology (such as data platforms) or processing and analytic services, are deeply embedded in the collection and use of patient data. The sharing of data, including patient's identifiable data, seems questionable in some circumstances and appears to be governed (in the case of data sharing within the DDS) by those sharing the data!

There seems, if not reluctance, then little thought given to encouraging meaningful public engagement, such as providing access to the papers or meetings of committees and other bodies that make important decisions about data use. Transparency materials explaining data use to the public are largely incomprehensible to those without some previous understanding. All in all, it is unclear how the public can hold the ICB to account for the misuse of confidential patient information. We also suspect that lack of resources, including for staff and staff training, pose a risk to patient confidentiality, but have no conclusive evidence for this.

Beyond SEL, our experience of public engagement events about the use of health and care data suggests that there is general support for the use of NHS data for public benefit (albeit with certain provisos), but concern about the private sector accessing and profiting from our data, at least without our consent.[62]

Our research suggests that confidential patient information, although apparently protected by legislation and the common law duty of confidentiality, can in many circumstances be legally accessed for purposes beyond patient care, provided that certain assurances are given. Moreover, as the letter from the NDG and CGCC indicates, some organisations are not following the letter of the law. This may be because of a lack of clarity: for instance, there is some controversy about whether CPI can legally be processed for purposes such as PHM without individuals' explicit consent. But there are also indications that patients' data is being accessed or processed without meeting the conditions laid down for its use (for example, the list of Risk Stratification Approved Organisations has only 24 ICB entries and there is no table available for Population Health Analytics). The Data Protection and Digital Information Bill 2 (2023), if passed, will remove a swathe of existing protections.

For now it seems that the most effective way of countering the growing access to our data is by understanding and insisting on the protections that we still have, and demanding transparency from those using our data: if those responsible for the use of our health data are aware that the public is monitoring them, it may at least help to ensure that they carefully consider their actions.

---

61 https://goodjobsfirst.org/introducing-violation-tracker/ accessed March 2023

62 The provisos and concerns are often downplayed in the reports on such events e.g. https://www.onelondon.online/wp-content/uploads/2022/09/Public-deliberation-in-the-use-of-health-and-care-data.pdf

Useful resources

Consent and confidential information. NHS England Transformation Directorate February 2023 https://transform.england.nhs.uk/information-governance/guidance/consent-and-confidential-patient-information/#ig_professional

The Information Commissioner's Office https://ico.org.uk

National Data Guardian https://www.gov.uk/government/organisations/national-data-guardian

An explanation of data and digital terminology. https://keepournhspublic.com/wp-content/uploads/2022/12/Digital-and-data.-Terminology-and-definitions-Dec22.pdf

NHS Data Sharing. A non-commercial website run by a GP with extensive experience as a Data Protection Officer, Caldicott Guardian, Data Privacy Officer and more. https://www.nhsdatasharing.info

Types of data

Identifiable – information that contains personal details that identify individuals such as name, address, email address, NHS Number, full postcode, date of birth.

Pseudonymised – individual level information where individuals can be distinguished by using a coded reference, which does not reveal their 'real world' identity, although the more data sets are combined, the more information accrues about an individual and the easier it becomes to identify them.

Anonymised – in theory, data which is about an individual but from which the individual cannot be personally identified. However, proposals within the Data Protection and Digital Information Bill, for example, suggest that data controllers may in future have the discretion to decide when personal data can be classified as 'anonymous', depending on the circumstances and resources available to an organisation. Significantly, anonymised data is not covered by data protection safeguards.

Glossary

BIU	Business Intelligence Unit
CGCC	Caldicott Guardian Chair of Council
CCG	Clinical Commissioning Group
CLDC	Common Law Duty of Confidentiality
CAG	Confidentiality Advisory Group
CPI	Confidential Patient Information
DDS	Discovery Data Service

DPA	Data Protection Act
DUC	Data Usage Committee
FOI	Freedom of Information
HIE	Health Information Exchange
ICO	Information Commissioner's Office
IGSC	Information Governance Sub-Committee
IGARD	Independent Group Advising on the Release of NHS Data
ICB	Integrated Care Board
ICS	Integrated Care System
NDG	National Data Guardian
NDOO	National Data Opt Out
NHSE	NHS England
PHM	Population Health Management
PHMIB	Population Health Management and Inequalities Board
PCN	Primary Care Network
SDE	Secure Data Environment
SEL	South East London
SELSON	South East London Save Our NHS
SoS	Secretary of State
SUS	Secondary Use Services

KONP calls for:

- the potential of our health data to be used for the benefit of patients/citizens, not for profit;
- the stewardship of NHS data to rest with the NHS;
- proper state-funded investment for NHS technology development and training;
- sound governance of our data to maintain trust, with an independent regulator;
- meaningful citizenship engagement about data use;
- transparency on the use of data so we know who is using our data and for what purpose; and the right to opt out of third party access.