NHS Federated Data Platform
FCI Position Paper

Introduction

In January 2023 NHS England (NHSE) opened a **tendering process**[1] to procure a **Federated Data Platform (FDP)**[2] for the NHS. The anticipated contract value will be £360 million over five years with an option for two twelve-month extensions worth a further £120 million. The data platform will be owned and controlled by the NHS "to unlock the power of NHS data to understand patterns, solve problems, plan services for local populations and ultimately transform the health and care of the people they serve." The tender notice states that:

"NHSE will undertake a competitive tendering procurement to replace its existing COVID-19 Data platform with a data platform for NHSE and NHS bodies. The data platform will be a cloud-based Software as a Service (SaaS) solution, which will enable the use and sharing of data within a safe and secure environment."

NHSE have stated they "are not mandating the use of the platform" but it will be of benefit for Trusts and for Integrated Care Systems (ICSs) "to support use cases that they [ICSs] wish to adopt. Local Trusts and ICSs will have the autonomy to use the data platform to address their own key challenges and priorities"

"De-identified data will only flow to central platforms for specific, necessary and pre-agreed planning purposes (such as national reporting on vaccine uptake, to increase supply chain efficiency or to create benchmarks of good practice that can inform national policy) and in compliance with information governance principles and data protection law".

Health and care data collection and analysis for purposes beyond direct care has a long and sometimes difficult history - going back to the disaster that was **Care.data**[3] - which was abandoned in 2014, and the planned 2021 collection of GP Data for Planning and Research (GPDPR) – which is on pause. There can be little doubt about the value of these data collections for planning and research purposes, as demonstrated by the **Covid-19 data collection**[4] and described in the **Goldacre Review**[5]. However, it has proven impossible so far for Government to build data collection systems, free from controversy around data ownership, access, oversight and security, sufficient to overcome public and professional distrust. This paper explores the key issues of concern and suggests a set of key questions which should be addressed, if the Government and NHS is to demonstrate its transparency and trustworthiness in how it collects, uses and shares health and care data.

Ethics, governance and public attitudes to data sharing

The **8 Caldicott Principles**[6] remain as relevant as ever. Note the later addition of Principles seven & eight to the original six from 1997:

- **Principle 7**: The duty to share information for individual care is as important as the duty to protect patient confidentiality.

- **Principle 8**: Inform patients and service

FACULTY OF CLINICAL INFORMATICS

users about how their confidential information is used.

The National Data Guardian (NDG) was responsible for stopping the **Care.data**[3] programme in its tracks because of concerns about patient choice and how the public's healthcare data might be used and shared. However the NDG at the time (Dame Fiona Caldicott) made clear her support for **the collection and use of health and care data for secondary purposes**[7] including planning and research, providing there is trust, openness ("no surprises") and public engagement in the process, stating:

"Good information sharing is essential for providing safe and effective care. There are also important uses of information for purposes other than individual care, which contribute to the overall delivery of health and social care or serve wider public interests."

Dr Nicola Byrne, the current NDG, has also been clearly supportive of the use of health and care data for the public good, and she has recently posted a **blog specifically on the FDP**[8] which **balances support for using data while emphasising the importance of maintaining trust throughout this procurement, including noting the importance of upholding the NHSs core values.**

This approach has also been affirmed by various citizen juries that have tested proposals for health and care data sharing over the past few years. In 2021 **citizen juries**[9] looked at data sharing initiatives relating to the Covid-19 pandemic. The juries were all charged with answering the same set of questions, about what the future should be, and who should make that decision, for three pandemic data sharing initiatives enabled through the **2020 Covid-19 COPI Notices**[10] (which were withdrawn in July 2022). These were:

• **Summary Care Record (SCR) Additional Information**[11] - which was extended to include additional information on over 50 million people in England without explicit consent.

• **NHS Covid-19 Data Store and Data Platform**[12] - a new store of patient-related data created by NHSE in response to the pandemic, with a wide range of software tools for planning and monitoring the pandemic and to support the delivery of the Covid-19 vaccination programme.

• **OpenSAFELY**[13] – a tool created at the start of the pandemic by the University of Oxford and with the backing of NHSE for pandemic-related research, using data accessed from GP patient records but with aggregated data outputs.

Overall, the juries supported the introduction of the initiatives during the pandemic. They were most supportive of the decision to introduce **OpenSAFELY**[13] (77% of jurors very much in support) and least supportive of the decision to introduce the **NHS Covid-19 Data Store and Data Platform**[12] (38% of jurors very much in support). Whilst supportive, many jurors were concerned that there was a lack of transparency about the data sharing initiatives, and in particular with the **NHS Covid-19 Data**

Store and Data Platform[12] and **Summary Care Record (SCR) Additional Information**[11] initiatives. The juries thought transparency and governance important even in a pandemic. Most jurors considered **OpenSAFELY**[13] to be the most transparent, trustworthy, and secure of the three data sharing initiatives. Very few jurors wanted decisions about the future of these data sharing initiatives to be taken by the minister or organisation accountable for the initiative (only 6% overall). Most believed that an independent body of experts and lay people should review the data sharing initiatives.

The University of Manchester in partnership with The Patients Association, recently published their pilot study from two focus groups on the **General Practice Data Trust**[14], prompted in response to the GPDPR. The research examined what patients thought about sharing their health data generally, and particularly about GPDPR. **They found that many participants had very low levels of trust in the Government and the NHS, with participants worried about the accuracy of their NHS records, the NHSs motives in gathering healthcare data for planning and research and particularly about possible uses of their data, by Government, pharmaceutical companies, or the insurance industry**. **However, patients were not opposed to sharing data for research and service improvement purposes, but they wanted more information on what would happen to their data if they shared it and how their data would be kept safe.**

The Federated Data Platform (FDP)

The **Federated Data Platform (FDP)**[2] is the latest attempt to access health and care data into secure data environments, for a range of purposes, including elements of direct care as well as secondary use purposes such as healthcare planning and research. On behalf of NHSE, Dr Timothy Ferris and Ming Tang recently posted **a blog on the FDP**[15]. In it they state:

"NHS England intends to procure a **Federated data platform (FDP)**[2], which is an ecosystem of technologies and services to be implemented across the NHS in England. This will be an essential enabler for transformational improvements across the NHS. The **FDP**[2] will enable, and must apply, secure data environment policy for any use of NHS health and social care beyond direct patient care. For example, when using data to support population health management and operational planning. This procurement will also support integrated care systems to implement secure data environment policy."

In his review, **Goldacre**[5] made clear that good research can be done with access to linked data sets without organisations needing to hold the data itself via Trusted Research Environments (TREs). The **Goldacre**[5] review recognised the **critical importance of minimising the risk of data duplication, assuring data quality, clinical safety, interoperability, and of reliable data curation.**

FACULTY OF CLINICAL INFORMATICS

The Department of Health & Social Care's (DHSC) **Data Saves Lives: reshaping health and social care with data**[16] report develops these ideas. Improving public trust in the health and care system's use of data is at the forefront of the proposals, for example, to establish **Secure Data Environments**[17] (SDEs) as the default route for NHS and adult social care organisations to provide access to their de-identified data for research and analysis.

In presentations to key stakeholders, the NHSE **FDP²** team have emphasised that the **"privacy by design"**[18] principle underpins their proposals. NHSE emphasise that the **FDP²** is a platform designed to facilitate data sharing rather than data collection, and it will be up to individual users (e.g. ICSs) to decide how to use it. **Data Protection Impact Assessments (DPIAs)**[19] have been undertaken, for the overall project, the procurement and each of its main stages, but we understand they have not yet been finalised. The **DPIAs**[19] merit scrutiny when published to ensure that privacy by design components are explicitly identifiable. Ideally, they should also point to the need for local use **DPIAs**[19] to be completed and published to ensure legal and ethical compliance, alongside local oversight, accountability, and transparency.

It should be emphasised that the centralised collection of GP data is not part of the **FDP²** project at this stage although it may well be included in the future. However, there would be nothing to prevent individual ICSs from deciding to include GP data on their own initiative, as it is clearly essential for local health and care planning. There is no direct relationship between the **FDP²** and the Secure / Trusted Research Environments already established (see below).

To fulfil their own data requirements, ICSs will need GP data and are therefore likely to invest in their own platform solutions alongside the **FDP²** to provide the range of data they need. **There is a risk that this may result in duplication of data and effort with consequent impact on resources, data curation and data security, with local variations in the interpretation and application of information governance and oversight requirements.**

There are also concerns that some GPs may not have the competence or capacity to fulfil their full responsibilities as data controllers, with a variety of local, regional, national and supplier specific collections already taken for wide-ranging purposes. The main GP system suppliers, EMIS and TPP, notionally act as data processors for tens of millions of lifelong patient records, supporting **OpenSAFELY**[13], ICS, and Primary Care Network (PCN) functions that are far from transparent, both to GP data controllers and their patients. Questions around GP supplier **"data lakes"**[20] and their data controllership issues, have been asked and are still unclear.

FDP Procurement

The **FDP²** is planned to integrate data across health and care systems to facilitate better care for patients including those with chronic conditions, improved population health, better planning of health and care services and find

new ways to deliver services.
The procurement is split into four lots:

- Platform procurement.
- Privacy enhancing technologies.
- Marketplace and training.
- Implementation and deployment.

Palantir Technologies[21] is an American software company that specialises in big data analysis, who already provide services in support of the Covid-19 vaccine programme to the NHS. While **Palantir Technologies**[21] are considered the front runners, they may be joined in the **FDP**[2] procurement process by other major technology companies.

Concerns about the FDP proposals

MedConfidential[22] and **Foxglove**[23], are two of the most high-profile critics of the current **FDP**[2] proposals. **MedConfidential**[22] has recently published the **first**[24] of a series of articles on "The Palantir Procurement". **MedConfidential**[22] has been consistently opposed to the various approaches NHSE have taken from **Care. data**[3] days onward. It is not opposed to data collections per se (see their **review of the first Goldacre Review**[25]) but rather the approach that NHSE seems to take, the procurement process, lack of clarity around process and purpose, risk of supplier lock-in and the high and **escalating cost**[26] (est. £360m to £480m). It also cites concerns about NHSE proposals to use the **FDP**[2] to support direct care where the use cases are a complex mixture of cohort management, public health, population health interventions

and individual care.

The GP community have long been wary of centralised data collections for purposes beyond direct care, reflecting both their status as data controllers and their common law duty of confidence to patients. **Helen Salisbury in a thoughtful BMJ article**[27] outlined a range of doubts about the **FDP**[2].

At its conference on 22 November 2022, the **British Medical Association (BMA)**[28] GP Committee expressed concern about any single supplier solution for **FDP**[2] that might result in vendor lock in:

"Federated Data Platform

(12) That conference notes with concern NHSEs plans to procure a £360m contract for a Federated Data Platform from a single supplier, raising questions over the safety of patient data and the oversight of any company that might potentially seek to exploit that data. In order to maintain the highest level of public trust this conference calls on the **BMA**[28] to work with NHSE to:

(i) Determine if the four existing secure data platforms supported by the **BMA**[28] /**The Royal College of General Practitioners (RCGP)**[29] Profession Advisory Group can provide some or all of the requirements of the proposed platform.

(ii) scrutinise organisations submitting tenders to ensure a demonstrable positive track record on security, privacy, and ethics.

FACULTY OF CLINICAL INFORMATICS

(iii) mitigate from the outset against vendor lock-in and ensure the commitments to modern, open working methods from the 13 June paper Data Saves Lives and 6 September paper on Secure Data Environments, both of which draw on the **Goldacre**[5] review, are enshrined.

Proposed by Mark Coley, GPC England Outcome - Carried"

The four Trusted Research Environment (TRE) platforms referred to in the **BMA**[28] GP Committee motion above were:

1. **NHS Digital's**[30] TRE
2. **OpenSAFELY**[13] in EMIS/-TPP,
3. **ONS (Office for National Statistics) TRE**[31]
4. **Genomics England's TRE**[32]

Data access and oversight

NHS Digital (NHSD) has been collecting **NHS activity data**[33] for many years, including GP data through its **GPES service**[34] for a variety of purposes including payments. **Independent Group Advising on the Release of Data (IGARD)**[35] was established by NHSD in 2016 to provide independent advice and recommendations on applications for the release of patient data into secure environments for research, audit and planning purposes. For GP data, **RCGP**[29] & **BMA**[28] jointly provided nominees to a GPES **Professional Advisory Group (PAG)**[36] whose purpose was to gain feedback from the **RCGP**[29] & **BMA**[28] on data sharing applications received by NHSD that included requests for GPES data for pandemic planning and research. Such

feedback was documented and forwarded to **IGARD**[35] as part of the original application for data.

From 1st February 2023, **Statutory Regulations**[37] were laid out and accepted by Parliament to dissolve NHSD and transfer its powers and responsibilities to NHSE. Within the regulations it states that the Secretary of State must publish guidance for NHSE about the exercise of the inherited data functions. The explanatory memorandum to the regulations makes clear that this guidance should cover how it takes independent expert advice. However, there seems to be some uncertainty about the future of **PAG**[37] & **IGARD**[35] after NHSD is incorporated into NHSE from 1st February 2023. NHSE's proposals require it to establish an independent **Data Advisory Group (DAG)**[38] "… that can, individually and collectively, provide expert advice and assurance on both internal and external access to data for purposes other than direct care". However, there are concerns that the new **DAG**[38] may not replicate the full independence of **IGARD**[35]. The draft statutory guidance is not yet finalised. There have been concerns expressed about the removal of a fully independent group (by NDG, peers, **IGARD**[35], **BMA**[28] and **MedConfidential**[22]). Recently in a House of Lords debate, **the minister appeared to say**[39] that independent oversight would remain after all. On a more positive note, the draft statutory guidance does make clear that advice should be taken on dissemination AND internal data use.

Independent scrutiny will continue to be provided by the NDG, and NHSE "must have

regard to any advice" given to it by the Health Research Agency's (HRA) **Confidentiality Advisory Group (CAG)**[40] . However, **CAG**[40] has a tight and restricted remit that may not cover much of the potential data use from the **FDP**[2]. It is not clear that there will be any ongoing independent scrutiny that includes professional representative bodies, such as the **BMA**[28] & **RCGP**[29] or independent patient representation.

It is still unclear what level of oversight and independent scrutiny will be applied to the FDP - either to internal NHSE uses or access to data held in the FDP. This is an important unknown when assessing the risks and benefits of the project.

Leadership, transparency and trust

The NHS has been trying to get better access to all health and care data for years, but successive projects have failed, generally on the back of lack of public trust in Government, particularly public unease about whether NHS data might be used for purposes that are not obviously publicly beneficial. There seems to have been a lack of clear, committed, and consistent sponsorship for the programmes from the DHSC and NHSE. This fits with the recent report from the House of Commons Health and Social Care Committee's Evaluation of Government commitments made on the digitisation of the NHS **(Fourth Special Report of Session 2022-23)**[41], which examined nine commitments across four broad policy areas. The overall rating was **inadequate** across all commitments with the roll-out of integrated

health and care records, de-identifying data collected from GPs and digital workforce development rated particularly poorly.

The fact that commercial partners are often involved in the infrastructure of data collections is not so obvious to people. The public is not well-sighted on the procurement process and may well have concerns about large foreign multinationals supplying critical infrastructure and support to the project.

Patients are not opposed to sharing data for research and service improvement purposes but want to know how it will be used and shared. Fundamentally patients want to understand how their data will be kept safe. It is clear that the public can and do support secondary uses of their data providing there is clear public benefit, their data is protected and not used for commercial purposes.

Successive NDGs have also supported this approach, emphasising the need for trust, transparency, and engagement. The benefits case has been made and reinforced by the success of the Covid-19 data collection & the **Goldacre**[5] Review. But there are staunch opponents of the NHSE approach. There is also anxiety and deep scepticism in the GP community about data sharing for purposes beyond direct care, though a number of data-sharing initiatives seem to be well-developed at ICS level and some national flows are well-established (e.g., GPES). The proposals so far formulated for the **FDP**[2] are unlikely to assuage GP concerns. Unfortunately, the positions of the various proponents are pretty well entrenched, and these perspectives may well

be irreconcilable in terms of developing and agreeing a mutually acceptable solution to the data uses and collection problem and its latest incarnation in the **FDP**[2].

NHSE could consider to at least take steps to make their position more defensible and transparent. The Citizen Jury report referenced above, made clear recommendations for actions which NHSE could take alongside the NDG's recently published **Public Benefit Guidance**[42] that could help NHSE demonstrate their commitment to ensuring data is used for public benefit in a transparent way. It seems that the **FDP**[2] may enable data use compatible with the 7th Caldicott Principle, but so far there is little evidence that the 8th Caldicott Principle has been satisfied. There is also professional uncertainty about applying these Principles in terms of population health and cross-organisational care. Certainly, citizens need to be able to understand unequivocally what their data can and will be used for, and what it will not be used for, unless subject to additional protections such as explicit consent or opt-out.

Summary

Overall there is a general lack of transparency about many aspects of the **FDP**[2] which is reminiscent of the recent history of **Care. data**[3], GPDPR and not made any easier by continuing NHS reform. There is a need to build trust by taking concrete action on privacy and transparency; trust cannot be earned through communications and public engagement alone. One approach that could ameliorate matters would be to start with a set of tightly controlled purposes, with clear constraints,

communications, and oversight, at national and locality level, defining what will and will not happen to healthcare data. Public trust could be built through such an approach, reflecting the federated data business model, and making it easier to define an appropriate platform ecosystem and demonstrate supplier conformance with standards. **Simply put, NHSE should tell people what they are planning to do and then listen.**

There are tests that can be applied to ensure that any proposed solution meets the technical (**Goldacre**[5]), legal & ethical (NDG) requirements for healthcare data use for individual, and population care, planning and research. Reconciling plans for any centralised data collection with the views of the clinical professions, particularly GP data controllers, critics such as **MedConfidential**[22], **Foxglove**[23] and the wider public, is likely to remain both a considerable obstacle and challenge for NHSE and Government. It will be very important to obtain much greater clarity and understanding about all of the above matters in order to build that vital public and professional trust upon which the success of this project is so dependent.

With all of the above in mind, in the appendix below, we have set out a list of questions, grouped under five headings, which we believe must be satisfactorily answered in order to clarify:

- The purposes and scope of the **FDP**[2].
- The oversight required at local and national level to build public and professional trust in the programme.

Appendix 1: Questions to help define the purpose, scope, and governance requirements for the FDP.

A. Dept. Health & Social Care / NHSE issues

a. Who is the SRO for the FDP Programme and who is the sponsor within the DHSC?

b. What lessons have been learned from the Care.data debacle and the GPDPR program that are relevant to the FDP program?

c. How has DHSC / NHSE organisational culture changed to make a successful and publicly acceptable deployment of the FDP more likely?

d. Describe the use-cases for the FDP in terms of:

    i. individual care,
    ii. cohort management,
    iii. public health,
    iv. population health interventions,
    v. other healthcare planning purposes
    vi. and research?

B. Information Governance issues

a. What oversight arrangements are in place nationally and locally to build public and professional trust, and provide evidence of accountability, and transparency?

b. When will you publish the full set of DPIAs for the FDP, ensuring details of privacy by design components are readily identifiable?

c. Are local use DPIAs being completed and published to ensure legal and ethical compliance, alongside local oversight, accountability, and transparency?

d. How has the NDG Public Benefit Guidance, outputs from the Citizen Juries and feedback from the General Practice Data Trust been incorporated into the design, development, and implementation of the FDP?

e. How do the governance proposals for the FDP satisfy the Caldicott Principles?

C. Data issues

a. When will the FDP include access to GP data?

b. What is the future for the GPDPR program?

c. What measures are in place to remove any unnecessary data duplication, assure data quality, clinical safety, inter-operability, and data curation in relation to the FDP?

d. How will the proposed SDEs interact with the established TREs?

D. Customer issues

a. Who are the planned customers for the FDP?

b. Will ICSs, PCNs and other organisations need to build systems duplicating some FDP functionality to continue to get access to essential GP data?

E. Procurement issues

a. Why have the DHSC / NHSE not adopted an open procurement approach to the FDP?

b. How do DHSC / NHSE intend to ensure that the FDP procurement does not result in single-supplier lock-in?

c. How will the FDP procurement be consistent with the Goldacre recommendations?

References

1   https://bidstats.uk/tenders/2023/W02/790495477

2   https://www.gov.uk/government/publications/secure-data-environment-policy-guidelines/secure-data-environment-for-nhs-health-and-social-care-data-policy-guidelines

3   https://www.bbc.co.uk/news/health-26259101

4   https://transform.england.nhs.uk/key-tools-and-info/data-saves-lives/improving-health-and-care-services-for-everyone/the-nhs-covid-19-data-store-putting-data-at-the-centre-of-decision-making/

5   https://www.gov.uk/government/publications/better-broader-safer-using-health-data-for-research-and-analysis

6   https://www.gov.uk/government/publications/the-caldicott-principles

7   https://www.gov.uk/government/speeches/national-data-building-trust-across-health-and-social-care

8   https://www.gov.uk/government/news/in-pursuit-of-balance-unlocking-the-power-of-data-whilst-preserving-public-trust

9   https://arc-gm.nihr.ac.uk/media/Resources/ARC/Digital Health/Citizen Juries/Broken Files/12621_NIHR_Juries_Report_ELECTRONIC.pdf

10   https://www.gov.uk/government/publications/coronavirus-covid-19-notification-of-data-controllers-to-share-information

11   https://digital.nhs.uk/services/summary-care-records-scr/additional-information-in-scr

12   https://www.england.nhs.uk/contact-us/privacy-notice/how-we-use-your-information/covid-19-response/nhs-covid-19-data-store/

13   https://www.opensafely.org/

14   https://www.pslhub.org/learn/commissioning-service-provision-and-innovation-in-health-and-care/health-records-and-plans/general-practice-data-trust-gpdt-pilot-study-report-on-patient-focus-groups-31-january-2023-r8675/

15   https://www.england.nhs.uk/blog/better-insights-better-decisions-better-health/

16   https://www.gov.uk/government/publications/data-saves-lives-reshaping-health-and-social-care-with-data/data-saves-lives-reshaping-health-and-social-care-with-data

17   https://www.gov.uk/government/publications/secure-data-environment-policy-guidelines/secure-data-environment-for-nhs-health-and-social-care-data-policy-guidelines

18   https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/

19   https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

20   https://medconfidential.org/2017/what-is-nhs-englands-national-data-lake/

21   https://www.palantir.com/uk/

22   https://medconfidential.org/

23   https://www.foxglove.org.uk/who-we-are/

24   https://medconfidential.org/2023/the-palantir-procurement-part-one/

25   https://medconfidential.org/2022/goldacre1/

26   https://www.computing.co.uk/news/4062533/gbp360m-nhs-federated-platform-tender

27   https://www.bmj.com/content/380/bmj.p292

28   https://www.bma.org.uk

29   https://www.rcgp.org.uk/

30   https://digital.nhs.uk/blog/inside-story/2022/tres-in-the-nhs---how-health-data-sharing-is-saving-lives

31   https://www.ons.gov.uk/aboutus/whatwedo/statistics/requestingstatistics/secureresearchservice

32   https://www.genomicsengland.co.uk/research/research-environment

33   https://digital.nhs.uk/data-and-information/data-tools-and-services/data-services

34   https://digital.nhs.uk/services/general-practice-gp-collections

35   https://digital.nhs.uk/about-nhs-digital/corporate-information-and-documents/independent-group-advising-on-the-release-of-data

36   https://digital.nhs.uk/coronavirus/gpes-data-for-pandemic-planning-and-research/gpes-data-for-pandemic-planning-and-research-profession-advisory-group-terms-of-reference

37   https://www.legislation.gov.uk/ukdsi/2023/9780348242690

38   https://www.gov.uk/government/publications/draft-guidance-on-nhs-englands-protection-of-patient-data/draft-guidance-on-nhs-englands-protection-of-patient-data

39   https://parliamentlive.tv/event/index/af1c5ad1-7862-414f-87e2-a276f1d-525d4?in=19:49:42

40   https://www.hra.nhs.uk/about-us/committees-and-services/confidentiality-advisory-group/

41   https://committees.parliament.uk/committee/81/health-and-social-care-committee/publications/

42   https://www.gov.uk/government/publications/what-do-we-mean-by-public-benefit-evaluating-public-benefit-when-health-and-adult-social-care-data-is-used-for-purposes-beyond-individual-care

Acknowledgements

FCI

FACULTY OF CLINICAL INFORMATICS

6 Alie Street, London, E1 8QT

fci.org.uk

info@fci.org.uk

faculty-of-clinical-informatics

@ukfci