Classification: Official

Publication reference: PRN00179

Protecting and safely using data in the new NHS England

26 January 2023, Version 1

In February 2023, NHS Digital will merge with NHS England. NHS Digital has responsibility for designing and operating national data infrastructure and digital systems. It safely and securely collects, analyses, and disseminates data from health and adult social care services in England and in some cases, Wales, Scotland and Northern Ireland. NHS England also collects, analyses and disseminates data from health services.

The government will use the powers in the Health and Care Act 2022 to make regulations to transfer the statutory functions of NHS Digital, to NHS England.

NHS England will become the single executive non-departmental government body with responsibility for digital technology, data and health service delivery in the NHS.

NHS England will assume responsibility for all activities previously undertaken by NHS Digital. This includes running the key national IT systems which support health and social care, as well as the collection, analysis, publication and dissemination of data generated by health and social care services, to improve outcomes.

This is a guide explaining how NHS England will continue to be an effective and secure guardian of public data, when it assumes responsibility for these activities.

What will the transfer achieve?

Data powers our NHS and is key to understanding and improving our services. It drives innovation and research, helps us to reduce inefficiencies and health inequalities and improves patient outcomes.

The merger follows a recommendation in Laura Wade-Gery's review, Putting data, digital and tech at the heart of transforming the NHS (November, 2021).

This merger will reduce duplication, bringing the NHS's national data and technology expertise together into one organisation. This will enable a closer link between the collection and analysis of data, and the delivery of service improvements as a result of that insight.

This document is organised around the following five promises:

NHS England as a data safe haven: our five data promises

1. NHS England will only use data to help deliver better services and outcomes for patients.

2. People can have confidence that their choices will be honoured and that their data is protected, secure, respected, and used appropriately.

3. NHS England will ensure its staff are trained and supported to maintain the highest standards of data protection, reinforced by robust data management processes and governance.

4. NHS England will operate with transparency and accountability. It will obtain independent, expert advice to oversee and assure its role as a data safe haven.

5. NHS England will use best-in-class technology and will continue to innovate to support data security.

1. NHS England will only use data to help deliver better services and outcomes for patients

Data managed by health and social care services can help to transform our health and care system and is essential to improving outcomes.

We will use data, and we will allow others to securely access data, to support four different outcomes:

- To deliver high-quality care to individuals.
- To understand, protect, and improve the health of the population.
- To effectively plan, evaluate, and improve the delivery of services.
- To research and develop innovative preventions, diagnostics, treatments, vaccines and other interventions, and monitor their impact on patient care.

NHS England will be the custodian of national datasets generated by health and social care services. It will assume NHS Digital's role of bringing data together, at a national level, and managing it securely and responsibly for the purposes described above.

It will also take responsibility for ensuring that the data is made available to approved users to improve health and care, where there is an appropriate legal basis, and where they demonstrate they can use the data safely. Examples include research to develop new treatments, or greater clinical understanding of health conditions and diseases; supporting population health; and facilitating health and adult social care planning and service commissioning.

More streamlined, safe, secure access to data by health and care providers will enable NHS England to promote the effective and efficient planning, development and provision of health and adult social care services.

NHS England will also take responsibility for publishing and continuously reviewing the open datasets and official statistical products that NHS Digital produces, in line with its publication obligations and the Code of Practice for Statistics. NHS England recognises this data is key to transparency and improving understanding of the NHS's services and operations.

Individual services will remain data controllers for patient health records and for collecting, storing, and managing access to the data that they need to care for patients and deliver local services.

2. People can have confidence that their choices will be honoured and that their data is respected, secure, protected and used appropriately

We will uphold the highest standards of data management, in terms of how we store, secure, analyse, manage, and allow internal and external access to data.

The same rules that applied to NHS Digital about collecting data, and making it available for research and analysis, will apply to NHS England. The transfer of statutory functions will include all existing protections for data.

We know that patient data is special and sensitive, and we will continue to respect that in the way that we protect and secure data, limit identifiability and manage access to it, including internal NHS England access to data. We will ensure that it is used to improve health and care.

We will be transparent about the use of data and will publish details of organisations who have been allowed access to data, the data they have accessed, the purpose for that access and the data they have used. We will also publish details about data obtained under the transferred NHS Digital functions which is accessed by NHS England.

This will provide the same level of transparency about internal access to the data as there was when NHS England accessed data from NHS Digital, before the merger. We will publish information about the independent advice we receive about internal and external data access and the decisions that are made.

We will have clear rules and processes to ensure that decisions about internal and external data access and use are made within a clear information governance framework, that processes are subject to assurance and scrutiny, and there is appropriate oversight by the board.

For all access to data for planning, commissioning and research purposes, we will:

- always default to de-identified data where we can – many uses of data do not require personal identifiers; we will therefore only use identifiers when essential
- not allow data to move out of our systems unless absolutely required – nearly all uses of data in the future will be inside secure data environments.

Respecting choice – trust and patient data opt-outs

NHS England will continue to uphold opt-outs in line with national policy and will ensure patients have a genuine choice about how their own identifiable data is used for purposes beyond their direct care.

We know from our research that the existing opt-out system is confusing and can be difficult to navigate for some people. The Department of Health and Social Care (DHSC) will work with NHS England, the National Data Guardian and other stakeholders to ensure patients have confidence in the opt-out system, and to ensure data continues to support the functioning of the health and care system.

NHS England will also continue to build awareness and increase transparency and trust in the way that data is used in the NHS. Increasing transparency and trust will be essential.

3. NHS England will ensure its staff are trained and supported to maintain the highest standards of data protection, reinforced by robust data management processes and governance

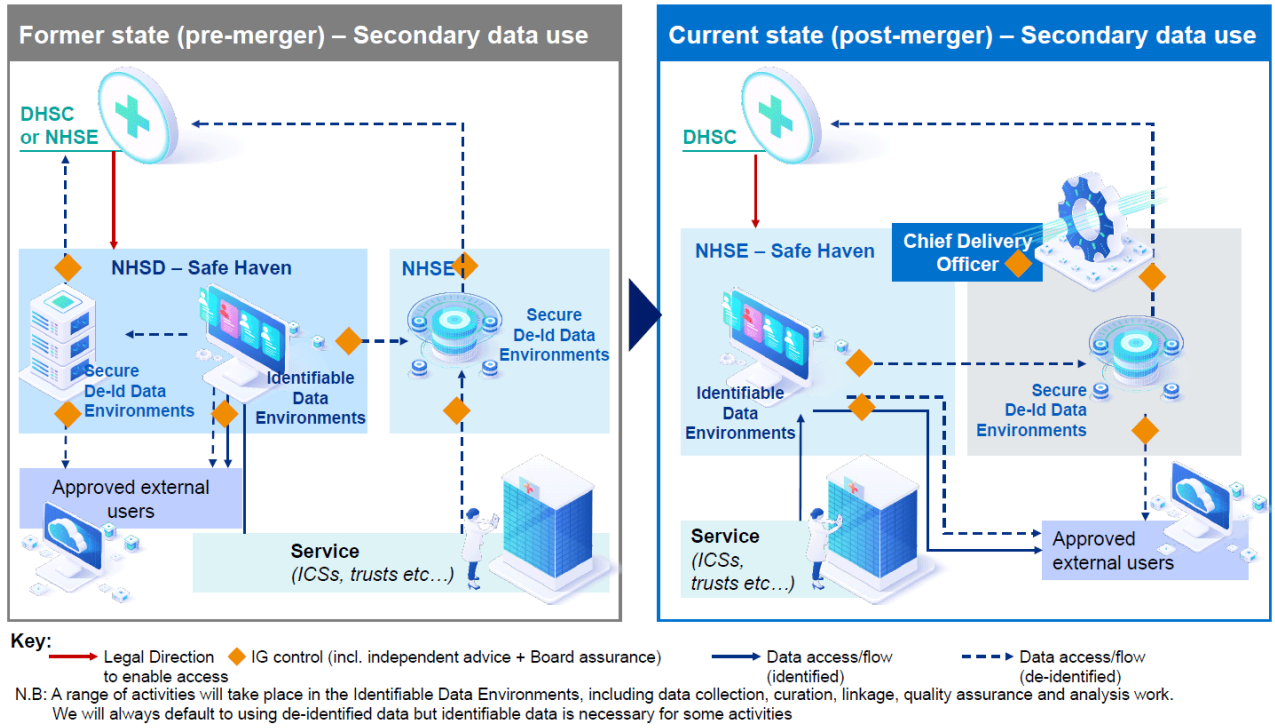
NHS England's robust policies and procedures, backed by staff training and support, will continue to enhance a culture of safe and secure data management, in which data is only used safely, securely, and appropriately, to deliver improved health outcomes.

NHS England will continue to have governance in place to ensure that the board, with its independent non-executive members, will oversee how NHS England exercises its new transferred data functions and protects patient data. It will also put in place arrangements for the independent scrutiny of internal and external data access and will obtain independent advice on its data collection and internal and external access processes.

Within the organisation, the chief delivery officer, as the senior information risk officer (SIRO), will have overall responsibility for NHS England's information risk policy. The information governance function and data protection officer will be part of the chief delivery officer's directorate. Together with the cyber security function and the Caldicott Guardian function, they will provide assurance on the protection of patient data and the appropriateness of its use.

The Transformation Directorate will lead the organisation's use of data and analysis, reporting to the national director of transformation; this is a separate part of the organisation to the delivery directorate. This will ensure separation of executive director accountability for information governance from operational aspects of data storage, data flows, and data use (see Figure 1 below). It also means that monitoring, auditing and assurance of data functions is undertaken by those with no role in the management or use of data.

Figure 1: Pre and post-merger data flows



This diagram shows the way that data flows and access were managed before the merger and how that will change as a result of the merger. In time, secure data environments (SDEs) will become the default way that users are provided with access to NHS data, including for NHS England analysts. More information on SDEs can be found in Section 5

4. NHS England will operate with transparency and accountability. It will obtain independent expert advice to oversee and assure its role as a data safe haven

Transparency will be key to maintaining public confidence in how NHS England obtains, holds, uses, disseminates, and protects data.

NHS England will, as NHS Digital did previously, publish all directions received from the Secretary of State so there is full transparency about the IT systems it delivers on behalf of the Secretary of State and about what data is being collected and analysed and for what purpose. It will also continue to publish requests made by other organisations for it to collect and analyse data.

Before establishing any new data collection, NHS England must consult with a variety of people, including representatives of those from whom information will be collected and those who may use the data.

Like NHS Digital, NHS England will publish information on its website about how it collects, uses and shares data with others, including a Data uses register . This will ensure that the public know what data is being shared, with whom and why. Organisations will only be allowed to access data if they have the right legal basis, can demonstrate that they can manage it securely and are using it to improve health and care.

NHS England will, as NHS Digital does, obtain independent advice on its data access processes, procedures and, where appropriate, on individual decisions around data access. This will also include its internal data access processes.

NHS England will put in place a new data advisory group to include independent advisers, including members of the previous NHS Digital Independent Group Advising on Release of Data (IGARD). This group will, individually and collectively, provide expert advice and assurance on both internal and external access to data for planning, commissioning and research purposes.

NHS England will consult with DHSC and the national data guardian on the terms of reference of the data advisory group, which will be approved by the NHS England Board and published.

NHS England will be required to report to Parliament, as part of its annual report, on how effectively it has discharged its new transferred data functions. This will include how it has protected patient data.

The information commissioner and the national data guardian are both key external stakeholders in relation to how NHS England uses, manages and protects patient data. NHS England will engage proactively and transparently with them to obtain their advice and challenge, in addition to engaging with them in their formal statutory, and in the case of the information commissioner's office, regulatory roles. It will also consult the national data guardian as part of producing its annual report.

NHS England will continue to manage the production of official statistics about health and care data, publishing these in line with the Code of Practice for Statistics, under the independent leadership of the organisation's chief statistician.

It will also continue to publish a wide range of open data, management information and statistical publications in accordance with its transferred data functions. In line with the Code, the chief statistician will have sole authority for deciding on methods, standards and procedures, and on the content and timing of official statistics. The chief statistician will report to the national statistician (the government's head of the statistical service) on all professional matters.

Taken together, all of this adds up to ensure that NHS England is upholding the highest standards of transparency and continues to be publicly accountable for how it collects, analyses, publishes and shares information.

5. We will use best-in-class technology and will continue to innovate to support data security

NHS England will ensure it has the right technologies in place to protect data and to enable the effective delivery of its services.

Secure data environments

SDEs are data storage and access platforms that will allow the NHS to provide approved users to access and analyse data, without it having to leave the environment. The technology will allow data access to be fully controlled and auditable, reducing the possibility of data misuse or theft. SDEs will enable the high-quality research and analysis to take place to improve outcomes, while upholding the highest standards of privacy and security.

SDEs will become the standard way that the NHS provides approved users with access to health and care data for planning, commissioning and research, including within NHS England. This change will greatly increase the level of protection in place. NHS SDEs will be designed to the highest standards, adhering to the SDE Policy Guidelines and designed with reference to the 'Five Safes' framework developed by the Office for National Statistics (ONS):

- Safe settings: the environment prevents inappropriate access, or misuse.
- Safe data: information is protected and confidentiality maintained.
- Safe people: those accessing the data are well trained, and authorised, to use it appropriately.
- Safe outputs: any summarised data taken away is checked to ensure it protects privacy.
- Safe projects: the use of the data goes through rigorous checks and approvals.

Some parts of the NHS are already using SDEs to a high standard; the NHS is investing significantly to build these platforms and adapt old systems over the next three years. This includes NHS England.

Cyber security

From the merger date, NHS England will take on responsibility for running critical national infrastructure for the NHS, supported by the existing dedicated cyber security capability that protects and monitors the systems and information in its care. Like NHS Digital before, NHS England will continue to work closely with the National Cyber Security Centre to understand the threats and manage the security risks. It will also have wider responsibility for the cyber-resilience of the NHS.

More specifically, NHS England will have several cyber security responsibilities:

- Managing the security risks to NHS England data
  - by running a dedicated cyber security function.
- Enabling the wider NHS to reduce cyber risk
  - by delivering capability to prevent, detect and respond to cyber events and ensure broader cyber resilience.
- Continually and strategically improving services and the overarching risk
  - by dynamically altering centrally delivered cyber services, information and support as threats evolve.
- Leading improved cyber outcomes in NHS England and the system
  - by regular board level engagement.

Annex A

Transfer regulations and statutory guidance

Regulations made by the Secretary of State under the Health and Care Act 2022, and subject to Parliamentary approval, will transfer NHS Digital's statutory functions to NHS England and abolish NHS Digital. This means that from the merger date NHS England will be responsible for discharging these functions. Under a separate transfer scheme, all of NHS Digital's assets, liabilities, contracts and staff will transfer to NHS England.

The transfer regulations contain specific provisions which impose additional requirements on NHS England in relation to how they will be required to discharge the new, transferred data functions:

- A requirement to have regard to Statutory Guidance which the Secretary of State issues about the exercise by NHS England of the transferred data functions.
- A requirement to publish information in its annual report about how effectively it has discharged the transferred data functions.

Statutory guidance

The statutory guidance will provide guidance to NHS England on measures the organisation should take to protect confidential information when exercising the transferred data functions, so as to ensure NHS England acts as a safe and effective guardian of people's data collected from NHS and adult social care services. This includes:

- Ensuring that its governance supports the provision of a safe haven for data, reflecting the accountability of NHS England's Board for the exercise of the transferred data functions.

- Ensuring responsibilities and accountabilities for functions that are managing and using data, for example for analysis and planning, are organisationally separate from the functions providing assurance and advice, such as information governance and Caldicott Guardian functions.

- Having processes and procedures in place for obtaining independent advice. This includes establishing a specific data advisory group to include independent advisers who can, individually and collectively, provide expert advice and assurance on both internal and external access to data for planning, commissioning and research purposes.

- Putting in place arrangements for engaging with key stakeholders in relation to the exercise of its transferred data functions.

- Internal processes to facilitate regular review and discussion with devolved governments in relation to information systems established for devolved governments, their bodies or agencies.

- Ensuring various technical measures and controls continue to be in place to protect data and arrangements continue to be in place to ensure data processing arrangements comply with UK GDPR.

- Operating with the same degree of transparency as NHS Digital did in relation to the collection, analysis, publication and use of data and ensuring the same degree of objectivity and transparency over the publication of data, including data on the performance of NHS services, in line with its transferred data functions and the Code of Practice for Statistics.

- Providing information in its annual report (for the first full year it exercises those functions and in subsequent years) about the steps taken by NHS England to follow the statutory guidance and to protect confidential information generally.

Directions to establish information systems

All existing directions to NHS Digital will become functions of NHS England to discharge as if they were directions made by the Secretary of State to NHS England. This includes directions previously made by NHS England. NHS England will have no power to direct itself to set up data collections using the transferred data functions. All future directions to NHS England to collect data using these functions will only be made by the Secretary of State.

Where directed by the Secretary of State, NHS England will be able to require information from health and adult social care bodies (and those providing services for them), and request data from any other organisation where this is necessary for it comply with a direction. NHS England will continue to minimise the burden of their requests for data on providers.

Publication of information

NHS England will be required to publish data it has collected and analysed under the transferred data functions unless it is exempt from doing so, including where it is prevented from doing so by law (for example if the data made patients or users identifiable).

Completely anonymous statistical data will continue to be published online for open access, including official statistics and management information and a range of statistical publications, in line with the Code of Practice for Statistics.

Data sharing

NHS England will only be able to share data where it has a legal power to do so and will not be able to provide access to or share confidential patient data unless the recipient has a legal basis under the common law duty of confidentiality to receive and process it. This means that NHS England may only share identifiable patient data:

- for the direct care of the patient (with consent implied)

or:

- where a patient has expressly consented

or:

- where there is a statutory gateway or legal requirement

or:

- where there is an overriding public interest justification.

NHS England will have processes for organisations to make for access to data for planning and research purposes. These will be subject to rigorous information governance requirements, to ensure the requesting organisation is accessing and using the data for appropriate purposes, sharing complies with UK GDPR and that data is protected and kept secure

Where a request involves access to confidential information, the requester may need to have express patient consent or support from the Confidential Advisory Group (an independent body which provides expert advice on the use of confidential patient information) for approval under regulation 5 of the Health Service (Control of Patient Information) Regulations (for example when it is impractical to obtain consent and another legal basis to meet the common law duty of confidence isn't in place). The principle of patient choice to opt-out will be applied in line with national policy where confidential data is requested.

A data sharing agreement (DSA) will be required where an external organisation is accessing record-level data which NHS England has collected under the transferred data functions, setting out the requirements for security, use, and destruction.

This means that data will be collected appropriately, stored safely and securely, and only accessed and shared for appropriate, beneficial purposes, respecting the privacy of individuals.

Compliance with data protection legislation

NHS England will continue to ensure all its procedures and activities are fully compliant with the existing UK laws relating to the protection of people's data, including the UK General Data Protection Regulation , the Data Protection Act 2018), and the Common Law Duty of

Confidentiality. This also includes complying with the Caldicott Principles when collecting, using and sharing confidential patient data. More information on Data Protection Legislation can be found on the Information Commissioner's website.