# Advanced AI Assessment

Data Management

Introduction

Access to health data is necessarily complex as it requires safeguards, high levels of security and data minimisation to mitigate the risk of re-identification and clear controls to ensure it is used only for appropriate purposes.

Source: NHS, (2019), Artificial Intelligence: How to get it right – Putting policy intro practice for safe data-driven innovation in health care care

Typology of data

- **Identifiable data** – "data where an individual can be identified either directly from the dataset or in combination with other datasets" (NHS, 2019, p. 44)

- **Anonymous data** – "Data in a form that does not identify individuals and where identification through its combination with other data is not likely to take place" (NHS, 2019, p. 44)

- **Synthetic data** – "A synthesised, representative dataset which does not relate to any real people" (NHS, 2019, p. 44)

Access to data
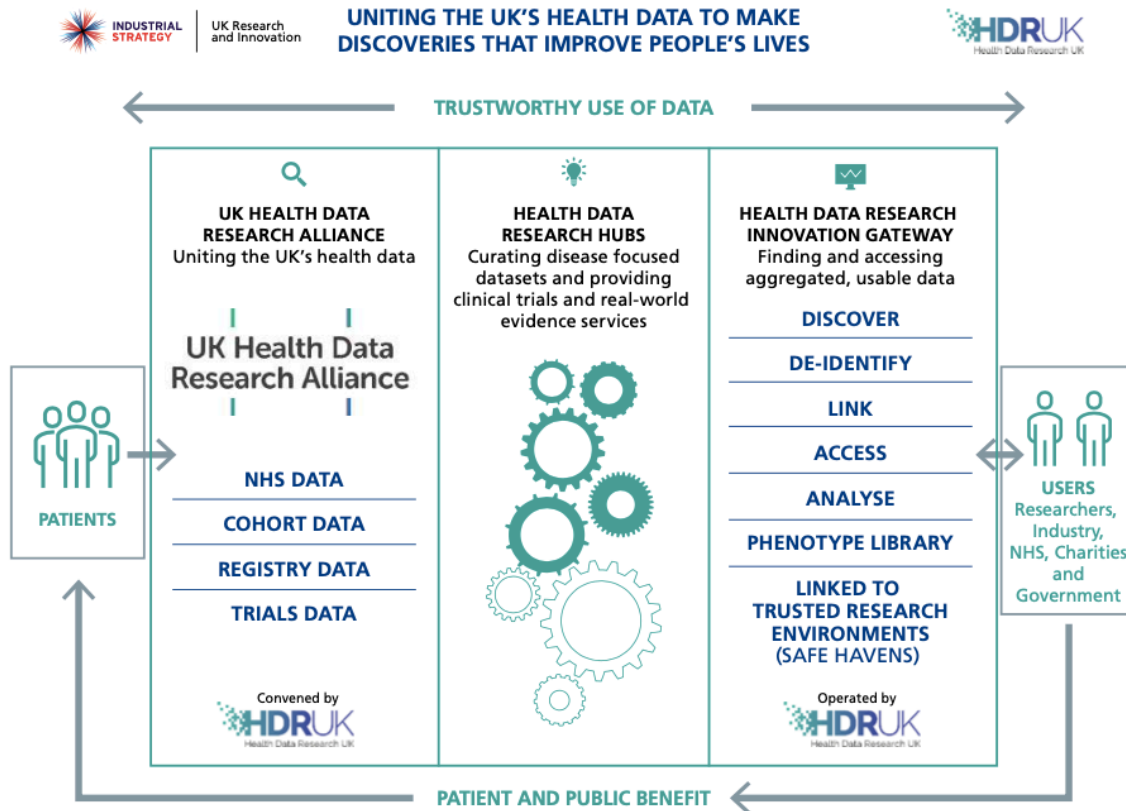
NHSX Data Framework

Principle 1

- Any use of NHS data, including operational data, not available in the public domain must have an explicit aim to improve the health, welfare and/or care of patients in the NHS, or the operation of the NHS. This may include the discovery of new treatments, diagnostics, and other scientific breakthroughs, as well as additional wider benefits.
- Where possible, the terms of any arrangements should include quantifiable and explicit benefits for patients which will be realised as part of the arrangement.

Principle 2

- NHS data is an important resource and NHS organisations entering into arrangements involving their data, individually or as a consortium, should ensure they agree fair terms for their organisation and for the NHS as a whole. In particular, the boards of NHS organisations should consider themselves ultimately responsible for ensuring that any arrangements entered into by their organisation are fair, including recognising and safeguarding the value of the data that is shared and the resources which are generated as a result of the arrangement.

Principle 3

- Any arrangements agreed by NHS organisations should not undermine, inhibit or impact the ability of the NHS, at national level, to maximise the value or use of NHS data. NHS organisations should not enter into exclusive arrangements for raw data held by the NHS, nor include conditions limiting any benefits from being applied at a national level, nor undermine the wider NHS digital architecture, including the free flow of data within health and care, open standards and interoperability.

NHSX Data Framework

Principle 4	• Any arrangements agreed by NHS organisations should be transparent and clearly communicated in order to support public trust and confidence in the NHS and wider government data policies.
Principle 5	• Any arrangements agreed by NHS organisations should fully adhere to all applicable national level legal, regulatory, privacy and security obligations, including in respect of the National Data Guardian's Data Security Standards, the General Data Protection Regulation (GDPR) and the Common Law Duty of Confidentiality.

Thank you