RESEARCH AND COMMERCIAL USE OF HEALTHCARE DATA IN THE UK

FUTURE CARE CAPITAL

A review of the legal issues surrounding the potential ownership and exploitation of healthcare data.

May 2020

Anthony Collins
solicitors

CONTENTS

EXECUTIVE SUMMARY

a. There are concerns that the interests of the commercial and public sectors are unfairly balanced under the existing legislative framework governing the use and exploitation of health care data, at times leading to valuable data sets being shared at an undervalue and putting individuals' rights and freedoms at risk. Whilst there are some legal obligations and regulatory guidance which emphasises the need to strike a 'fair deal', there is a significant gap in recommendations which outline how this can be achieved in practice. Data controllers need to be conscious that their decisions and actions have a direct impact on the current and potential value of any personal data they control.

b. There is a legal and regulatory gap which leaves data controllers exposed: they are required to protect the financial value of the personal data they hold and the commercial opportunities created by medical research without proper explanation of how that value is to be calculated.

c. There is a common misconception that the Courts will readily supplant the decisions of a public body with their own. The Courts cannot quash or declare unlawful a decision merely on the basis that the judge would have reached a different conclusion (e.g. set a different price). Whilst the Courts may conclude that a public authority decision is invalid on the grounds of illegality, procedural unfairness, and irrationality; it is the market which is the ultimate arbiter of 'value', not the Courts, and why the state seeks to encourage healthy and competitive markets.

d. As a result, legal action concerning the use of health data will generally be limited to breach of a data or intellectual property rights (concerning the data subject or the intellectual property owner respectively) or a failure to follow due process (by the public body sharing or exploiting the data) but, the Courts are not the appropriate forum to determine the 'value' of health data in monetary terms.

e. The starting point in any proposed use of personal data is for each party to 'get its house in order'. This requires understanding and complying with the law around the rights of individuals and the criteria that must be satisfied to carry out data processing activities. This forms the basis of **Part 1** of this report and focusses on the rights of the individual: different types of personal data, legal grounds for processing it and the role of consent in healthcare information governance.

f. The legal issues surrounding medical research are some of the most complex to navigate. This is due to several factors including:

    - the newly enhanced and developing area of personal data rights;
    - the technical specialism of managing intangible assets / intellectual property rights as distinct from the control of data in and of itself;
    - the multi-layered and often contradictory legislation applicable to the NHS;
    - the political sensitivities surrounding the NHS, its unique access to large-scale, sensitive data and concerns about its current and future funding model.

g. Once organisations understand what data they hold in respect of individual data subjects, there is then an opportunity to combine it and process the resulting data set. Processing data on this larger scale can create new challenges to the rights of data subjects and broader, public duties must be considered. **Part 2** of this report looks at managing data sets and the impact that human rights may have upon organisations' use of personal data.

h. Effective management of data can lead to the creation of new data sets which could have significant value as intangible assets. The data sets and the scientific progress created by their analysis is commercially exploitable or may otherwise be offered, shared and used for a public benefit. **Part**

3 of this report discusses the potential for health data to become an intangible asset and the framework in which this value could / should / must be realised.

To assist with your navigation of the report, we have summarised the role of different organisations which work together to process data along with short descriptions of the organisations forming part of the NHS governance matrix.

RESPONSIBILTY FOR DATA

DATA CONTROLLER

- Controllers are the main decision-makers – they exercise overall control over the purposes and means of the processing of personal data. Controllers shoulder the highest level of compliance responsibility – they must comply with, and demonstrate compliance with, all the data protection principles as well as the other GDPR requirements.
- They are also responsible for the compliance of their processor(s). The controller is responsible for assessing that its processor is competent to process personal data in line with the GDPR's requirements. A controller must only use a processor that can provide "sufficient guarantees" (in terms of its expert knowledge, resources and reliability) to implement appropriate technical and organisational measures to ensure the processing complies with the GDPR and protects the rights of individuals (Article 28(1) of GDPR).
- Once the controller has chosen a suitable processor, it must put in place a contract or other legal act that meets all the requirements of Article 28(3) of GDPR and give the processor documented instructions to follow (either in the contract or separately). Controllers should ensure a processor's compliance on an ongoing basis, in order for them to satisfy the accountability principle and demonstrate due diligence.
- A controller will be liable for any damage (and any associated claim for compensation payable to an individual) if its processing activities infringe the GDPR. However, a controller will not be liable for damage resulting from a breach of the GDPR if it can prove it was not in any way responsible for the event giving rise to the damage.

DATA PROCESSOR

- Processors act on behalf of, and only on the instructions of, the relevant controller. A processor may make its own day-to-day operational decisions, but Article 29 of GDPR says it should only process personal data in line with a controller's instructions.
- A processor may be contractually liable to the controller for any failure to meet the terms of their agreed contract. In addition to the contract terms, a processor also has some direct responsibilities and liabilities under the GDPR.
- If a processor is involved in the processing which infringes GDPR, the individual making the claim for compensation can claim against either party. A processor can be held liable under Article 82 of GDPR to pay compensation for any damage caused by processing, including non-material damage such as distress. It will not be liable if it can prove it is not responsible for the event giving rise to the damage. If a processor is required to pay compensation, but is not wholly responsible for the damage, it may be able to claim back from the controller, the share of the compensation for which they are responsible.

JOINT DATA CONTROLLERS

- If two or more controllers jointly determine the purposes and means of the processing of the same personal data, they are joint controllers. However, they are not joint controllers if they are processing the same data for different purposes (see Data Controllers in Common below).
- All joint controllers remain responsible for compliance with the controller obligations under the GDPR. Both supervisory authorities and individuals may take action against any controller regarding a breach.
- Joint controllers are joint and severally liable. Each joint controller will be liable for the entire damage caused by the processing, unless it can prove it is not in any way responsible for the event giving rise to the damage
- Joint controllers are not required to have a contract, but you must have a transparent arrangement that sets out your agreed roles and responsibilities for complying with the GDPR.

DATA CONTROLLERS IN COMMON

- Data controllers in common share a pool of personal data that they process independently of each other but do not jointly determine the purposes and means of the processing.
- Whilst often disclosing data to each other, each organisation will be processing the data independently of the other and so they are not expected to be held liable for each other's breach.
- As with 'joint' arrangements, data controllers in common should have written agreements and processes for ensuring that all data controller responsibilities are satisfied.

Department of Health & Social Care	Executive Agencies	**Medicines and Healthcare Products Regulatory Agency** has the specialist role of assessing, licensing and regulating medicines and medical devices for use in the United Kingdom.
		Public Health England is responsible for delivering public health improvement, through prevention and awareness raising and protection and infection control.
	Executive non-departmental public bodies	**NHS England** oversees the NHS in England, commissions specialised healthcare services and primary care services and oversees Clinical Commissioning Groups.
		NHS Improvement which, from 1 April 2016, combines the roles of The **NHS Trust Development Authorit**y had the function of helping NHS Trusts achieve successful applications for Foundation Trust status **Monitor**, which oversaw Foundation Trusts and applications from NHS Trusts seeking foundation trust status. It also had the new role of examining pricing and competition in the NHS.
		The Human Tissue Authority regulates the use of human tissue in research and therapeutic treatments.
		Health Education England is responsible for ensuring enough high-quality training is available to develop the healthcare workforce.
		NHS Digital, which provides statistical information and informatics support to the health and care system.
		Care Quality Commission has the primary function of inspecting providers of health and adult social care in England, ensuring that they meet essential standards of safety and quality.
		The **National Institute for Health and Care Excellence**, 'NICE', which provides advice on treatment procedures and assesses healthcare interventions for cost-effectiveness.
		The **Human Fertilisation and Embryology Authority**, which regulates and inspects in vitro fertilisation, artificial insemination and the storage of human eggs, sperm or embryos. It also regulates human embryo research.
		The **Health Research Authority** protects and promotes the interests of patients and the public in health research.
		NHS Blood and Transplant, which is responsible for the supply of blood, organs, tissues and stem cells; their donation, storage and transportation.
		The **NHS Business Services Authority** provides business support services to NHS organisations, including the administration of the NHS pension scheme
		NHS Resolution, handles negligence claims and helps the NHS learn lessons from claims to improve patient and staff safety.
		The **NHS Counter Fraud Authority**, tasked with leading the fight against NHS Fraud and corruption.

Please note: *We have not included NHSX as it is not a statutory-based body, but is instead equivalent to a government joint venture bringing together the techniacl expertise from the Department of Health & Social Care, NHS Improvemetn and NHS England.*

***Figure 1**: a summary of relevant bodies which connect with and influence the governance of NHS bodies, referred to within this report.*

PART 1 - RIGHTS OF THE INDIVIDUAL

WHAT IS PERSONAL DATA?

1.1. "Personal Data" means:

- any information "relating to an identified or identifiable living individual" (section 3 of the Data Protection Act 2018 (**DPA**)); and
- any information "relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person" (Article 4 of General Data Protection Regulations 2016 (**GDPR**)).

1.2. An individual is 'identified' or 'identifiable' if you can distinguish them from other individuals[1]. A combination of identifiers may be needed to identify an individual. If, by looking solely at the information you are processing you can distinguish an individual from other individuals, that individual will be identified (or identifiable). You don't have to know someone's name for them to be directly identifiable, a combination of other identifiers may be sufficient to identify the individual. Even if you may need additional information to be able to identify someone, they may still be identifiable.

1.3. Aggregated data (statistical data about several individuals that has been combined to show general trends or values without identifying individuals within the data), will not be personal. However, statistical analysis which concerns an individual or where the sample size is so small that the information can be disaggregated so that the natural person can be identified, will remain personal data.

1.4. The information 'relates to' a particular individual if you are processing it to learn or record something about that individual, or where the processing has an impact on that individual. Data can contain references to an identifiable individual, or be linked to them, but not 'relate to' them as it is not about that individual but is about another topic entirely. Depending on the circumstances, this data may or may not be personal data. When defining personal data, the Information Commissioners Office (**ICO**) gives the following examples:

- "a name and a corporate email address clearly relates to a particular individual and is therefore personal data. However, the content of any email using those details will not automatically be personal data unless it includes information which reveals something about that individual, or has an impact on them"[2]; whereas

[1] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/

[2] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/what-is-personal-data/

- medical history is "obviously about" an individual and is personal data "regardless of the purpose for which you are processing the data"[3].

1.5. You must have a valid lawful basis to process personal data. The six lawful bases are set out within Article 6 of the GDPR (consent, contract, legal obligation, vital interests, public task, legitimate interests). If no lawful basis applies to your processing and no exemption applies, your processing will be unlawful and in breach of the first principle under the GDPR – lawfulness, fairness and transparency.

Personal data: any information which enables a living person to be identified and informs you about that individual.

1.6. The DPA explains that "the GDPR's definition is more detailed and makes it clear that information such as an online identifier, for example a computer's IP Address, can be personal data. The more expansive definition expressly provides for a wide range of personal identifiers to constitute personal data, reflecting changes in technology and the way organisations collect information about people"[4].

1.7. In some circumstances there may be a possibility that someone might be able to reconstruct data generally in such a way that identifies an individual. When considering whether individuals can be identified, you may have to assess the means that could be used by an "interested and sufficiently determined"[5] person and this can place quite an onerous burden to satisfy[6]: the ICO refers to a 'motivated intruder' test.

1.8. You have a continuing obligation to consider whether the likelihood of identification has changed over time (for example as a result of technological developments). "Personal data that has been pseudonymised, for example key-coded data, can fall within the scope of the GDPR if it is still possible to attribute the pseudonym to a particular individual."[7]

1.9. Pseudonymised data can help reduce privacy risks by making it more difficult to identify individuals, but it is still personal data. If personal data can be anonymised, then the anonymised data is not subject to the GDPR or DPA (see below discussion whether true anonymisation can be achieved).

1.10. Information about a deceased person does not constitute personal data and therefore is not subject to the GDPR or DPA but may still be subject to the common law of confidentiality (see section 5 below).

---

[3] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/what-is-the-meaning-of-relates-to/

[4] Explanatory notes, paragraph 12 of DPA.

[5] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/

[6] *We are still waiting for the Supreme Court's judgment in WM Morrison Supermarkets plc v Various Claimants: Morrison's appeal against the Court of Appeal ruling that it was vicariously liable for its employee's misuse of data in the first successful UK class action for a data breach.*

[7] Explanatory notes, paragraph 12 of DPA.

WHAT IS SPECIAL CATEGORY DATA?

2.1. Personal data may also include special categories of personal data or criminal conviction and offences data. These are considered to be more sensitive and you may only process them in more limited circumstances. If you are processing special category data, you need to identify both a lawful basis for processing under Article 6 of GDPR and either obtain the individual's consent or satisfy another condition for processing in compliance with Article 9 of GDPR. Both consent and the other legal grounds for processing are discussed in more detail below.

2.2. "Special category data" or "Sensitive personal data" means:

- "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, genetic data, or of biometric data (for the purpose of uniquely identifying an individual), data concerning health, data concerning an individual's sex life or sexual orientation" (section 35 of DPA); and
- "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation" (Article 9 of GDPR).

Special category data requires heightened data protection measures due to its sensitive and personal nature.

2.3. These additional safeguards (requiring legal grounds under both Articles 6 and 9 of GDPR) are extended so that they specifically apply to data concerning health as well as genetic data, and biometric data, where processed in a way that uniquely identifies an individual.

2.4. We have considered below whether it is possible to anonymise genetic and biometric data. We have concluded that such data will always fall within the definition of personal data. When genetic and biometric data is also "processed for the purpose of uniquely identifying a natural person" it is subject to the additional safeguards granted by virtue of being special category data.

WHAT IS DATA CONCERNING HEALTH?

2.5. Data concerning health means:

- "personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status" (Article 4 of GDPR and section 205 of DPA);
- "all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject. This includes information about the natural person collected in the course of the registration for, or the provision of, health care services as referred to in Directive 2011/24/EU of the European Parliament and of the Council to that natural person; a number, symbol or particular assigned to a natural person to uniquely identify the natural person for health purposes; information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples; and any information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health

professional, a hospital, a medical device[8] or an in vitro diagnostic test" (Recital 35 of GDPR).

Data concerning health: Information relating to a natural person's past, current or future physical or mental health that reveals information about that person's health status.

2.6. "Data concerning health" qualifies as special category data (Article 9 of GDPR and section 35 of DPA) and it will therefore be necessary to satisfy legal grounds under both Articles 6 and 9 of GDPR in order to process data concerning health.

WHAT IS BIOMETRIC DATA AND HOW IS IT TREATED DIFFERENTLY FROM OTHER CATEGORIES OF PERSONAL DATA?[9]

3.1. Biometric data means:

- "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allows or confirms the unique identification of that natural person, such as facial images or dactyloscopic[10] data" (Article 4(14) of GDPR and section 205 of DPA 2018).

3.2. Biometric data qualifies as special category data (Article 9 of GDPR and section 35 of DPA) and it will therefore be necessary to satisfy legal grounds under both Articles 6 and 9 of GDPR in order to process biometric data.

Biometric Data: information generated from measurable human biological and behavioural characteristics, which can be used for identification.

3.3. The definition applies more broadly than taking biological samples for example, voice records which are processed through a Voice ID system are biometric data. It does not apply to all biological or behavioural information, for example the processing of photographs is only covered by the definition of "biometric data" when they are processed **through a specific technical means** allowing the **unique identification or authentication of a natural person** (Recital 51 of GDPR) such as facial-recognition software.

3.4. Biometric data is broader than genetic data which is "personal data relating to the inherited or acquired genetic characteristics of an individual which gives unique information about the

---

[8] *There is a question as to whether the definition of 'medical device' should be extended to incorporate algorithms and other technical methods of analysing personal data.*

[9] *Biometric data is also subject to additional safeguards elsewhere under the Protection of Freedoms Act 2012 which provides for the destruction, retention, use and other regulation of certain evidential material; to impose consent and other requirements in relation to certain processing of biometric information relating to children. The Protection of Freedoms Act 2012 is not relevant to processing biometric data for medical research.*

[10] *Dactyloscopy is the study of fingerprints.*

physiology or the health of that individual and which results, in particular, from an analysis of a biological sample from the individual in question" (Article 4(13) of GDPR and section 205 of DPA 2018): genetic data is a type of biometric data.

3.5. As a form of special category data, it will be necessary to satisfy legal grounds under both Articles 6 and 9 of GDPR in order to process biometric data.

Conclusions:

- Data which can identify a natural, living person and which enables you to learn or record something about an individual will be personal data. You must have a lawful basis to process personal data.
- Aggregate data and anonymised data is not personal data because it does not identify or relate to an individual.
- De-identified or de-personalised data is likely to fall within definition of pseudonymised data (see section 6 below).
- Special category data requires more protection because it is sensitive, the risk to the individual is greater if this type of data is processed inappropriately.
- Biometric data, genetic data and data concerning health will always constitute personal data.
- Biometric data and genetic data will qualify as special category data if processed for the purpose of identifying an individual.

PART 2 – CREATING DATA SETS

CAN INDIVIDUALS CONSENT TO DATA PROCESSING?

4.1. Historically, consent has provided the necessary legal authority for data processing activities and it remains one of the lawful bases for processing under Article 6 of GDPR. The requirement for valid consent has been enhanced under the GDPR and remains a key legal basis for processing special categories of personal data under the GDPR (Article 9(2)(a) of GDPR). Processing personal data and special category data can be lawful provided the individual has given clear and explicit consent for you to process their personal data for a specific purpose.

4.2. However, the GDPR sets a high standard for consent and confirms that 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 relating to him or her, such as by a written statement, including by electronic means, or an oral statement… Silence, pre-ticked boxes or inactivity should not therefore constitute consent." (Recital 32 of GDPR). Where relying upon consent, Article 7 of the GDPR places the burden of proof upon the data controller to evidence that the requirements have been met and great care must be taken to ensure that the consent is valid before relying on it as a lawful basis for processing.

4.3. Taking into account the different elements for establishing valid consent, it can be difficult to satisfy the legal requirements and, due to these challenges, another lawful basis may be more appropriate for processing health data. We address each of these challenges below.

When broken down into its constituent parts, consent is unlikely to be the appropriate legal basis for processing data for health and social care research.

Freely given

4.4. The ICO confirms that "public authorities, employers and other organisations in a position of power" may find it more difficult to satisfy the requirements for consent and should avoid relying on consent unless they are confident that they can demonstrate it is freely given[11]. However, consent should not provide a valid legal ground for the processing where there is a clear imbalance between the position of the data subject and the controller (or the processing is necessary for the performance of a contract – Article 7(4) of GDPR)), which renders it unlikely that consent was freely given in all the circumstances of that specific situation (Recital 43, GDPR).

4.5. A "clear imbalance" is not defined but the Health Research Authority (**HRA**) has published guidance which states that consent would not be appropriate "where the controller is a public authority and the data subject depends on their services, or fears adverse consequence, so

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

feels they have no choice but to agree"[12]. Even where consent is not bundled up as a condition of service, the issue for public authorities is that individuals might feel they have no choice but to agree or fear adverse consequences if they do not consent. The ICO recommends that "If you are a public authority or are processing employee data or are in any other position of power over an individual, you should look for another basis for processing, such as 'public task' or 'legitimate interests'."[13]

4.6. Nevertheless, the ICO does recognise that public authorities are not prohibited from relying upon consent and there may be situations where it can be shown that consent is freely given. It will be necessary to consider all the circumstances of the specific situation. As a result, timing can be key when asking individuals for consent to process their data. An obvious touchpoint for obtaining consent (for processing data for medical research) is when an individual is seeking or undergoing treatment or consent is being obtained in respect of their participation in a medical trial, but the individual's reliance upon or desire for that service could undermine the requirement that their consent is 'freely given'. Consent may be more appropriate where individuals are not currently or imminently dependent upon the services provided by the data controller, but regard must still be given to the intrinsic power imbalance between individual and health provider: individuals will be conscious that they may be dependent upon such services in the future.

4.7. One of the practical challenges with consent in a medical research context is that to be freely given, data subjects must also have the right to withdraw their consent at any time (Article 7(3) of GDPR). Consent is appropriate if you can offer people real choice and control over how you use their data and want to build their trust and engagement. Consent will not be valid where it cannot be withdrawn. If you would still process the personal data without consent, asking for consent is misleading and inherently unfair.

4.8. Relying upon consent as a lawful basis for processing presents a problem where the withdrawal of consent and the resulting removal of the personal data, would limit the validity of the research. The GDPR and DPA provide some exemptions which excuse researchers from complying with the individual's right to be forgotten[14] but this means that by asking individuals for their 'consent', they are given a false choice and only the illusion of control. As a result, when considering the overarching principles of fairness and transparency, another ground for processing is likely to be more suitable.

Informed & unambiguous indication

4.9. In addition to being "freely given", the consent must be "clearly distinguishable" from any other matters in a written document and be "in an intelligible and easily accessible form, using clear and plain language" (Article 7(2) of GDPR). For consent to be "informed", the data subject should be aware at least of: the identity of the controller, the purposes of the processing for which the personal data are intended and the processing activities. You must tell people who you are giving their information to, unless you are relying on an exception or an exemption. The ICO discusses the provision of granular consent so that individuals can

[12] https://www.hra.nhs.uk/planning-and-improving-research/policies-standards-legislation/data-protection-and-information-governance/gdpr-guidance/what-law-says/consent-research/

[13] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/when-is-consent-appropriate/

[14] Where data is processed for scientific research purposes - recital 65 of the GDPR,

consent to separate purposes or activities (unless this would be unduly disruptive or confusing). In the context of medical research, it may not be possible to identify all the purposes at the time the consent is originally sought.

If the request for consent is vague, sweeping or difficult to understand, then it will be invalid.

4.10. Informed consent also relies on individuals having the necessary expertise to understand the risks that may be involved in what they are consenting to. The data controller has a duty to explain to people what they are consenting to in a way they can easily understand. Evidence has shown that "providing the details of what we are consenting to is too complicated for the vast majority of people to understand"[15]. Furthermore, consent can "create bias in the data, often detrimental to already disadvantaged social economic groups who are more likely to refuse or withdraw consent" [16] (especially when asked for retrospectively).

You need to keep your consents under review and refresh them if your purposes or activities evolve beyond what you originally specified.

4.11. Data controllers will need to consider how they can best keep data subjects informed over the lifetime of the project as and when new technologies are developed, creating new processes and purposes for which the data could be used. The ICO states it is good practice to use a dashboard to let people manage who their data is sold to, or shared with, where they have a choice[17]. Aside from the administrative burden created by contacting individuals, it may be inappropriate to request updated consent from data subjects many years after their initial treatment has concluded and could lead to increased withdrawals of consent if they are contacted frequently after their original consent was given.

Specific

4.12. Where processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation. In addition, where the processing has multiple purposes, consent should be given for all of the purposes (Recital 32, GDPR).

4.13. It has been recognised that the problems with explicit consent for the use of patient data for health research are "often underestimated": new technologies mean that we are not yet aware of all the potential uses of data and it would not be practical or cost-effective to seek renewed

---

[15] The Right to Privacy (Article 8) and the Digital Revolution', Joint Committee on Human Rights 2019

[16] *'Patient data for health research: a discussion paper on anonymisation procedures for the use of patient data for health research' (Mr Evert-Ben Van Veen, October 2011)*

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

consent from patients, often years after their initial consent was given or after their medical treatment has ended[18].

4.14. Whilst the ICO has recognised that consent to process personal data for scientific research means that data controllers don't need to be as specific as for other purposes, you should still "identify the general areas of research, and where possible give people granular options to consent only to certain areas of research or parts of research projects".[19] Ultimately, the use of anonymised and pseudonymised data will enable data controllers to overcome the hurdles presented by relying upon consent and we have analysed below (at section 5) the alternatives to relying on consent.

Lack of capacity

4.15. "All consent must be opt-in consent, i.e. a positive action or indication and you may not rely on silence, inactivity, default settings, pre-ticked boxes or your general terms and conditions, or seek to take advantage of inertia, inattention or default bias in any other way"[20]. This can present particular challenges where the data subject lacks capacity and a registered Lasting Power of Attorney or Court appointed Deputy has not been granted explicit authority to give consent on their behalf.

4.16. Mental capacity is time and decision specific and it is important to remember that a person must be assumed to have capacity unless it is established that they lack capacity (section 1 of the Mental Capacity Act 2005). With this in mind, assessors should not take a blanket approach as capacity.

4.17. For example, it is not sufficient to state 'person [X] lacks capacity' but rather 'person [X] (on a balance of probabilities) lacks the capacity at this time, after taking all practicable steps to help them, to make the decision to do [Y]'. For example, a person may be able to consent to their data being processed for specific purposes but not to participate in a medical trial[21]. The burden of proving a lack of capacity to take a specific decision (or decisions) always lies upon the person who considers that it may be necessary to take a decision on their behalf.

4.18. It is unlawful to carry out intrusive research on or in relation to a person who lacks capacity to consent (section 30 of MCA). Research is "intrusive" if it is of a kind that would be unlawful if it was carried out on or in relation to a person who had capacity to consent to it, but without his consent.

Research on or in relation to a person is not legal where their consent is required, and they lack capacity to consent.

---

[18] 'Patient data for health research: a discussion paper on anonymisation procedures for the use of patient data for health research' (Mr Evert-Ben Van Veen, October 2011)

[19] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/what-is-valid-consent/

[20] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/what-is-valid-consent/

[21] *Please note this advice is concerned with the use of personal data in medical research. The consent requirements and specific regulations applicable to clinical trials falls outside the scope of our instructions.*

4.19. It is possible to continue using an individual's information for the purposes of the research project where that information or material was obtained before P's loss of capacity, the project follows an appropriate protocol and liaises with an appropriate person who is engaged in caring in the individual or interested in their welfare (Regulation 3 of the Mental Capacity Act 2005 (Loss of Capacity during Research Project) (England) and (Wales) Regulations 2007).

Consent to data processing is not the same as consent to participate in a medical trial, which is subject to separate legislation.

Children

4.20. Data protection law also contains specific protections for children. For the purposes of the GDPR, a child is someone below the age of 16, although Member States can reduce this age to 13, as the UK has done in the DPA. Therefore, consent to data processing can only be obtained from a child under 13 if the consent is authorised by a parent. In the UK, children who are 13 or older are expected to give consent in the same way as adults - with all of the associated risks. Other conditions under which the GDPR allows data to be processed can also be applied to children's data, although organisations may find the criteria for the 'legitimate interests' condition, in particular, difficult to meet in relation to children.

Problems with consent in the context of medical research

4.1. Consent is not inherently better or more important than other lawful grounds for processing, but it is attractive to data controllers as it can provide an easy way to evidence that the processing is in line with people's reasonable expectations. The consent process, whilst not perfect, aids transparency and fairness by setting out the proposed use of the data with data subjects.

4.2. The ICO has produced detailed guidance to explain why it may not be appropriate to rely upon consent as the primary legal basis for processing data in certain circumstances[22] for example, where it is not possible to demonstrate that consent is freely given, informed, unambiguous and specific. Consent "relies on us, as individuals, to understand, take decisions, and be responsible for how our data is used. But … it is difficult, if not nearly impossible, for people to find out whom their data has been shared with, to stop it being shared or to delete inaccurate information about themselves."[23] If consent is difficult, you should consider using an alternative legal ground.

4.3. The HRA and MRC have both concluded that consent is not likely to be an appropriate legal basis for processing data for health and social care research[24]. This is because "if you use consent as the legal basis for your processing and a participant withdraws their consent, you

[22] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/when-is-consent-appropriate/

[23] The Right to Privacy (Article 8) and the Digital Revolution', Joint Committee on Human Rights 2019

[24] https://www.hra.nhs.uk/planning-and-improving-research/policies-standards-legislation/data-protection-and-information-governance/gdpr-guidance/what-law-says/consent-research/ and http://www.highlights.rsc.mrc.ac.uk/GDPR/lawful_basis.html

will not have a legal basis to process personal data about them"[25]. This contrasts with other legal grounds where processing can continue despite the individual's objection or request to be forgotten (see below section 5).

4.4. Even when consent is given, all too often the limit of that consent is not respected."[26] For example, where individuals have knowingly consented to sharing some of their personal data, they may not be content with that data being combined to create a profile of themselves that they have no opportunity to see or edit. Considering the lack of accountability and limited resource of the ICO to bring enforcement action, there remains a power imbalance between individuals and data controllers across both the private and public sectors. Until individuals are empowered to take action or the industry imposes some form of self-regulation, data subjects cannot be confident that their consent creates genuine limitations on what data controllers can do with their data in practice.

4.5. Overall, if you cannot offer a genuine choice and data subjects are not empowered to control the use of their data, consent is unlikely to be the most appropriate ground: legitimate interests, or public task basis is more likely to be relevant.

Conclusions:

- Consent is unlikely to be the most appropriate lawful basis for processing personal data for the purpose of medical research when:
    - the individual doesn't really have a free choice to give or to refuse consent;
    - the individual feels any pressure to consent or has concerns over the consequences of refusing consent;
    - the individual does not understand the risks that may be involved in what they are consenting to;
    - it is difficult, if not nearly impossible, to contact data subjects when new purposes are identified or for people to find out whom their data has been shared with, to stop it being shared or to delete inaccurate information about themselves;
    - you will need to continue processing personal data after the individual has withdrawn their consent;
    - the limit of that consent is not respected.
- Other legal grounds may be more suitable (see: Section 5).
- Children and individuals without capacity (at the time their consent is sought) cannot meet the requirements of providing valid consent for data processing.
- Consent will still need to be considered in respect of complying with the common law of confidentiality and also the individual's participation in any medical research (not just in respect of data processing), see section 5 below.

[25] https://www.hra.nhs.uk/planning-and-improving-research/policies-standards-legislation/data-protection-and-information-governance/gdpr-detailed-guidance/legal-basis-processing-data/

[26] *'The Right to Privacy (Article 8) and the Digital Revolution', Joint Committee on Human Rights 2019*

WHAT ARE THE LEGAL GROUNDS AVAILABLE (FOR RESEARCH AND DEVELOPMENT) FOR PROCESSING HEALTH DATA WITHOUT CONSENT?

5.1. We have explained that consent is unlikely to be the most appropriate lawful basis for processing for health and social care research because the requirement for valid consent has been enhanced under the GDPR and will be very difficult to satisfy in the context of processing for medical research (see section 4 above).

5.2. Processing special category is prohibited unless another valid lawful basis can be satisfied in Article 6 of GDPR and at least one condition listed in GDPR Article 9. The legal basis that most research organisations used under the 1998 data protection legislation was processing to support 'legitimate interests'. Under GDPR:

- commercial companies and charitable research organisations will continue to use 'legitimate interests' as their legal basis (Article 6(1)(f) of GDPR) except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child; and
- universities, NHS organisations or other public authority processing personal data for research should be 'necessary for the performance of a task in the public interest' or 'exercise of official authority vested in the controller' (Article 6(1)(e) of GDPR).

Where organisations span both areas, the appropriate legal ground will depend on the actual processing – it is task specific as public bodies may carry out commercial activities which are not in the public interest, so would need to rely on legitimate interests. Each organisation will need to review its constitution to consider whether the processing falls within or outside the scope of the tasks it performs in the public interest.

Article 6 ground for lawful processing – legitimate interests

5.3. Private-sector or third-sector organisations will often be able to consider the 'legitimate interests' basis in Article 6(1)(f) of GDPR if they find it hard to meet the standard for consent and no other specific basis applies. This recognises that you may have good reason to process someone's personal data without their consent – but you must avoid doing anything they would not expect, ensure there is no unwarranted impact on them, and that you are still fair, transparent and accountable.

5.4. This can be broken down into a three-part test:

- **Purpose test:** are you pursuing a legitimate interest?
- **Necessity test:** is the processing necessary for that purpose?
- **Balancing test:** do the individual's interests override the legitimate interest?

5.5. The GDPR allows data controllers to now consider the legitimate interests of any third party, including wider benefit. The ICO confirms that "a wide range of interests may be legitimate interests. They can be your own interests or the interests of third parties, and commercial

interests as well as wider societal benefits. They may be compelling or trivial, but trivial interests may be more easily overridden in the balancing test."[27]

5.6. The ICO goes on to state that "you should avoid using legitimate interests if you are using personal data in ways people do not understand and would not reasonably expect, or if you think some people would object if you explained it to them. You should also avoid this basis for processing that could cause harm, unless you are confident there is nevertheless a compelling reason to go ahead which justifies the impact."

5.7. If you are processing special category data, in most cases the sensitive nature of this data means there are greater risks to the interests and rights or freedoms of the individual. You can still consider legitimate interests as your lawful basis, but you also need a special category condition under Article 9 for processing special category data.

5.8. Public authorities cannot rely on legitimate interests for any processing they do to perform their tasks as a public authority and should instead consider the 'public task' basis. This restriction on the use of legitimate interests is about the nature of the task, not the nature of the organisation.

Article 6 ground for lawful processing – public interest or official function

5.9. 'Task in the public interest' is similar to the pre-GDPR ground of processing for functions of a public nature and requires that the relevant task or function has a clear basis in EU or Member State law. 'Exercise of official authority' is satisfied if you can show that you are exercising official authority which is laid down by law (for example, a public body's tasks, functions, duties or powers), including use of discretionary powers. To fulfil its intention to provide the UK with universal effective health care, the NHS requires information and evidence based on the whole population and medical research at the population level can require access to large, representative samples of accurate patient and population data.

5.10. Whilst there does not need to be a specific statutory power to process personal data, the underlying task, function or power must have a clear basis in law. If you are exercising official authority, you do not need to satisfy any 'public interest' test but you must be able to demonstrate that the data processing is 'necessary' for that purpose: if you could reasonably perform your tasks or exercise your powers in a less intrusive way, this lawful basis does not apply.

You do not need specific legal authority for the particular processing activity. The point is that your overall purpose must be to perform a public interest task or exercise official authority, and that overall task or authority has a sufficiently clear basis in law.

5.11. You should document your lawful basis so that you can demonstrate that it applies. In particular, you should be able to identify a clear basis in either statute or common law for the relevant task, function or power for which you are using the personal data.

Article 9 ground for lawful processing - public interest, scientific or historical research purposes

[27] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/

5.12. The new legislation was written with research in mind and one of the additional conditions for holding and using special categories of personal data (for all organisations, public authority or otherwise) is Article 9(2)(j) of GDPR provided the processing is:

- **necessary** for archiving purposes, scientific or historical research purposes or statistical purposes;
- **proportionate** to the aim pursued;
- in the **public interest**; and
- subject to appropriate safeguards which protect the fundamental rights and the interests of the data subject (as outlined in Article 89 of GDPR).

5.13. Not all research is covered by this condition. You need to demonstrate that your research is either scientific or historical in nature, and in the public interest. This applies to both public-sector and private-sector research. It can include, for example, technological development and demonstration, fundamental research, applied research and privately funded research.

5.14. The term 'public interest' is not defined, but you need to point to a wider societal, rather than just your own interests (e.g. carrying out market research) or the interests of the particular individual. The HRA has noted that in order to serve the public interest, research sponsors will have to demonstrate that their research serves "the interests of society as a whole"[28]. When considering that our society operates on a pooled-risk model (through the NHS), it is generally recognised that scientific research is beneficial to the whole of society and forms part of our 'social contract' even where the outcomes of that research only directly benefits a group of individuals. However, the European Data Protection Supervisor has commented that the research should be carried out "with the aim of growing society's collective knowledge and wellbeing, as opposed to serving primarily one or several private interests."[29]

5.15. The legislation does not require that the 'public interest' overrides any commercial interest when relying on Article 9(2)(j) of GDPR. Indeed, the ICO confirms that "commercial scientific research may therefore be covered, but you need to demonstrate that it uses rigorous scientific methods and furthers a general public interest"[30].

5.16. Existing European case law confirms[31] that necessity and public interest implies 'a pressing social need' as opposed to largely private or commercial advantages. However, the European Data Protection Supervisor recognises that there has been a growing concern with the "blurring of the boundaries between public interest, academic freedom and private gain."[32]

---

[28] https://www.hra.nhs.uk/information-about-patients/

[29] https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf

[30] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-are-the-conditions-for-processing/#conditions7

[31] *Handyside vs the UK* App no. 5493/72 (ECHR, 7 December 1976); *Leander v. Sweden* App no. 9248/81 (ECHR, 26.03.1987)

[32] United Nations Conference on Trade and Development, Digital Economy Report 2019, September 2019; https://unctad.org/en/PublicationsLibrary/der2019_en.pdf?user=46

Until this lawful basis (processing for public interest, scientific or historical research purposes) has been sufficiently tested in case law or through enforcement by the ICO, what amounts to a 'public interest' will remain open to interpretation.

5.17. Whilst we await further guidance, regulatory action and judicial clarity on the definition of 'public interest', it is helpful to consider the ICO guidance which applies to "substantial public interests" (governed by Article 9(2)(g) of GDPR) and the circumstances in which it permits the processing of special category data[33]. In respect of substantial public interests, the ICO confirms that: "public interest covers a wide range of values and principles relating to the public good, or what is in the best interests of society. Commercial or private interests are not the same as a public interest... Of course, **you can still have a private interest - you just need to make sure that you can also point to a wider public benefit**….Given the inherent risks of special category data, it is not enough to make a vague or generic public interest argument – you should be able to make specific arguments about the concrete wider benefits of your processing. For example, you may wish to consider how your processing benefits the public in terms of both depth (i.e. the amount of benefit experienced from the processing, even if by a small number of people) and breadth (the volume of people benefiting from the processing)."[34]

Commercially driven research projects will be able to rely on Article 9(2)(j) as a lawful basis for processing; provided there is some public interest being pursued, the processing is necessary and proportionate, and the appropriate safeguards are implemented.

5.18. Once the necessity, proportionality and public interest elements of Article 9 have been satisfied, the data controller must then ensure the appropriate safeguards are implemented.

5.19. The safeguards outlined in Article 89 of GDPR (and discussed in Recital 156) concern data minimisation and pseudonymisation which are likely to be present in most scientific research already. Where processing for scientific research is in accordance with Article 89, the DPA 2018 includes an exemption from some provisions of the GDPR (for example the right of access) in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and so the curtailment of the data subject's rights are necessary for the fulfilment of those purposes (see above section 4 for a discussion on consent as a lawful basis for processing).

5.20. Despite some enhanced safeguards, data can be stored for research for long periods of time, and it is recognised that personal data collected for any initial purpose can be used for research. Researchers (acting as data controllers) can, for example, keep very long-term patient health data, refuse to delete personal data if the data subject withdraws their consent

---

[33] *This separate ground relates to a wide range of values and principles relating to the public good and confirms those reasons for processing which are either always or demonstrably in the best interests of society. A list of these interests can be found within paragraphs 6 to 28 Schedule 1 of DPA 2018.*

[34] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-are-the-substantial-public-interest-conditions/

for the research, and use data from one research project for others[35]. However, researchers can only use data from one research project for others if the new purpose is compatible with the original purpose, they obtain specific consent from data subjects for the new purpose, or they can point to a clear legal provision requiring or allowing the new processing in the public interest (for example, a new function for a public authority). If an organisation has collected data on the basis of legitimate interest, a contract or vital interests, it can be used for another purpose, but only after checking that the new purpose is compatible with the original purpose. If an organisation has collected the data on the basis of consent or following a legal requirement, no further processing beyond what is covered by the original consent or the provisions of the law is possible; further processing would require obtaining new consent or a new legal basis. Data controllers must also update privacy information to ensure that the terms and conditions applied to processing remain transparent.

5.21. The GDPR exempts research from the right to erasure insofar as it is "likely to render impossible or seriously impair the achievement of the [research] objectives" (Article 17(3)(d)). It may not always be clear when this exemption applies as both the research objectives and technology are likely to evolve over time, creating new opportunities and obstacles. Clearly, any ability for individuals to erase their personal data could have a significant impact on the validity of scientific findings in clinical trials, epidemiological studies and medical research, so understanding how this right and the accompanying exemption will apply in practice, will be crucial to not only the research but also to ensure the data doesn't become unduly limited or otherwise biased due to patient opt-out.

5.22. It might initially appear difficult to reconcile the GDPR's intention to enhance data subjects' rights and control over their personal data, with the ability for data controllers to nullify the right of erasure and to retain their personal data indefinitely. However, Recital 65 of the GDPR reiterates that, where processing the personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed (where a data subject has withdrawn his or her consent or objects to the processing of personal data), further retention remains limited to circumstances where the retention is necessary "for exercising the right of freedom of expression and information, for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, on the grounds of public interest in the area of public health, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or for the establishment, exercise or defence of legal claims." Necessity is the satisfying criteria for retention of data which would otherwise contravene the individual's rights.

5.23. When considering the above, there is a clear need to ensure appropriate safeguards are applied consistently across the sector to ensure they protect the fundamental rights and the interests of the data subjects, rather than act as a 'loophole' for compliance. Without a central body responsible for governing how NHS data is used, these safeguards and any curtailment of data subjects' rights are likely to develop on a piece-meal basis, causing inconsistencies in the market and confusion for individuals. Whilst NHSX is reviewing the current data governance of various NHS-bodies (With the National Data Guardian for Health and Social Care and the ICO), this is likely to take some time and there that many organisations will

[35] https://www.hra.nhs.uk/planning-and-improving-research/policies-standards-legislation/data-protection-and-information-governance/gdpr-detailed-guidance/safeguards/

already be working on projects which fall short of the required standards due to an absence of external control or agreed best practice.

Duty of confidentiality

5.24. Other parts of the law still require that consent is obtained before research can happen (e.g. Human Tissue Act, Medicines for Human Use (Clinical Trials) Regulations, etc.). It is important to remember that obtaining consent to take part in research and for disclosure of confidential information is still important and distinct from consent as a lawful basis for data processing. GDPR doesn't change this. The National Data Guardian has prioritised work which will seek to address the interplay between the requirements of common law and statutory data protection law[36] but this remains a complex area where the law and regulatory guidance has failed to keep up with the developments in health data.

5.25. To ensure their processing of patient data is lawful, data controllers must ensure:

- an Article 6 condition is satisfied (for personal data);
- an Article 9 condition is satisfied (for special category data); and
- they have complied with the common law requirements of confidentiality, for example there is consent or some other statutory authorisation for the data use (such as s251 of the NHS Act 2006).

5.26. Information is confidential if:

- it is not in the public domain (no such limit is placed on the definition of personal data);
- it can be related to an identifiable individual (similar definition of identifiable as used for personal data but, whereas personal data can only relate to a living person, confidential information can relate to the living or deceased[37]);
- it has a degree of sensitivity associated with it (no such element in the definition of personal data, but there is a similar consideration for special categories of personal data); and
- it is given with the expectation that it will be kept confidential. Individuals do not have to be explicit about their expectations, when entrusting others with their information: this expectation is often implicit, given the relationship the individual has with their doctor, nurse, researcher, etc.

5.27. Information can still qualify as 'confidential' after the individual has passed away.

Unlike personal data, confidential patient information also covers information related to deceased persons and so the duty of confidence will remain after death.

---

36 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/815950/1037_-_NDG_consultation_response_10.07.19_FINAL_TO_PUBLISH.pdf

37 *Lewis v Secretary of State for Health* [2008] EWHC 2196 (QB)

5.28. "Patient data is recorded so that it can be used by health and care professionals to care for patients, make diagnoses and decisions about the patient's care"[38]. This is referred to as 'for individual care and treatment', or 'direct care'. When an individual entrusts a research team, or a clinical care team, with confidential information, the team must handle this information in line with the patient's 'reasonable expectations'. Registered and regulated professionals (who are a part of the care team providing direct care through the care pathway) can rely on a patient's implied consent to share information as an integral part of the individual's consent to examination and treatment. The reliance of implied consent is only applicable within the context of providing the data subject with direct care.

5.29. Patient data is also used for purposes that go beyond an individual's care – to enable NHS organisations to understand the health needs of their local population, to monitor and manage services, and for research. This is referred to as 'secondary use' of data. Implied consent cannot be relied upon in the context of 'secondary use' and there must be some other statutory authorisation for the data use, such as medical research or matters of protecting public health or containing a global pandemic. Patients have the right to dissent from the disclosure of their personal confidential data for secondary purposes unless the law compels disclosure.

NHS opt-out: secondary-use of data

5.30. Patients and the public can now make an informed choice about whether they wish their confidential patient information to be used only for their individual care and treatment or also for secondary purposes beyond their individual care and treatment - such as commissioning, risk stratification, financial and national clinical audit, healthcare management and planning, research and public health surveillance[39].

5.31. Where a data subject opts-out of their confidential patient information being used for purposes other than their own care and treatment, the common law requirement on confidentiality must be considered and applied alongside existing data protection legislation, other laws and best practice.

5.32. When a patient has set a national data opt-out, organisations covered by the opt-out policy must make sure the patient's opt-out choice is respected. By March 2020 all health and adult social care organisations are required to be compliant with the national data opt-out policy, where they are using confidential patient information for purposes beyond an individual's care and treatment[40].

5.33. The national data opt-out applies to data that originates within the health and adult social care system in England[41]. This definition is aligned to section 250 of the Health and Social Care Act 2012 (**H&SC Act**) which defines the organisations required to have regard to published

[38] https://digital.nhs.uk/services/national-data-opt-out/understanding-the-national-data-opt-out/individual-care-and-research-and-planning-uses-of-data

[39] https://digital.nhs.uk/services/national-data-opt-out

[40] https://digital.nhs.uk/data-and-information/information-standards/information-standards-and-data-collections-including-extractions/publications-and-notifications/standards-and-collections/dcb3058-compliance-with-national-data-opt-outs

[41] https://digital.nhs.uk/services/national-data-opt-out/operational-policy-guidance-document/which-organisations-does-the-opt-out-apply-to

information standards. The national data op-out therefore applies to[42]: adult care homes, ambulance services, child health services, community services, Defence Medical Services (DMS), dentists (providing NHS care), DHSC and the national bodies it governs, GP practice, home-provided services, hospitals, mental health services, opticians (providing NHS care), pharmacists (providing NHS care), private providers including Any Qualified Providers (AQPs) who provide health and adult social care services which are funded or co-ordinated by a public body, public health services (including local authority services and providers such as school nursing), and secure facilities such as prisons and young offender institutes. The national data opt-out also applies to any subsequent release of the data collected by these organisations acting as data controllers, such as NHS Digital or Public Health England. Data relating to private care held by NHS Digital is included.

5.34. The national data opt-out does not apply to: health and care data for privately-funded care or treatment by a private provider organisation, unless it is coordinated by a public body, such as a local authority, organisations providing only children's social care, organisations that deal with health related data that originated outside the health and adult social care system, for example assessments for disability or other benefits purposes for the DWP, patient information that originated outside England, including home nations and crown dependencies - these locations may have their own opt-out arrangements and cross-border issues will need to be considered.

5.35. The opt-out applies when the purpose of the data use changes rather than when the data leaves the NHS organisation that collected the data. Therefore, a trust would need to apply the opt-out to patient data if its use changed from individual care to research. The national data opt-out does not apply to information that is anonymised in line with the Information Commissioner's Office (ICO) Code of Practice (CoP) on Anonymisation or, where it is aggregated or count type data[43]. Personal demographic data linked to clinical data, or drawn from a patient's medical record, is subject to the opt-out but demographic data not drawn from the medical record would not be subject to the opt-out. For example, a name and address on their own, without clinical information, is not classed as confidential patient information[44].

5.36. The national data opt-out does not apply where a patient has given their explicit consent to a specific use of their data. If a patient has agreed to a specific use of data, after being fully informed, then the national data opt-out does not apply. Even patients who have registered a national data opt-out can agree to take part in a specific research project or clinical trial, by giving their explicit consent. The national data opt-out also does not apply where law or regulation provides an exemption, which we discuss below.

5.37. In the UK there are legal avenues that allow the disclosure of confidential information to support medical research in compliance with the common law of confidentiality, even when this is not in line with the data subject's 'reasonable expectations' (i.e. direct care) and one of the main functions of the Health Research Authority is to approve the processing of

[42] https://digital.nhs.uk/services/national-data-opt-out/understanding-the-national-data-opt-out/who-must-comply-with-the-national-data-opt-out-policy

[43] https://digital.nhs.uk/services/national-data-opt-out/understanding-the-national-data-opt-out

[44] https://digital.nhs.uk/services/national-data-opt-out/operational-policy-guidance-document/appendix-6-confidential-patient-information-cpi-definition

confidential information relating to patients[45]. Where it is not practical to get explicit consent, section 251 of the NHS Act permits the common law of confidentiality to be set aside for specific secondary uses.

Section 251 approval: overriding the NHS opt-out

5.38. In England and Wales, section 251 of the NHS Act 2006 (originally Section 60 of the Health and Social Care Act 2001) provides the statutory authorisation to ensure that NHS patient identifiable information needed to support essential NHS activity can be used without the consent of patients. 'Essential', here, is the term used by the Medical Research Council as shorthand for medical purposes that are in the interests of patients or the wider public interest.

5.39. Section 251 approval can temporarily set aside the common law duty of confidentiality in research scenarios. Such disclosure of patient data, for 'secondary use' without consent, can be approved by the HRA who are advised by the Confidentiality Advisory Group (**CAG**)[46] whether there is sufficient justification to access data without consent. "The power can be used only to support medical purposes that are in the interests of patients or the wider public, where consent is not a practicable alternative and where anonymised information will not suffice."[47]

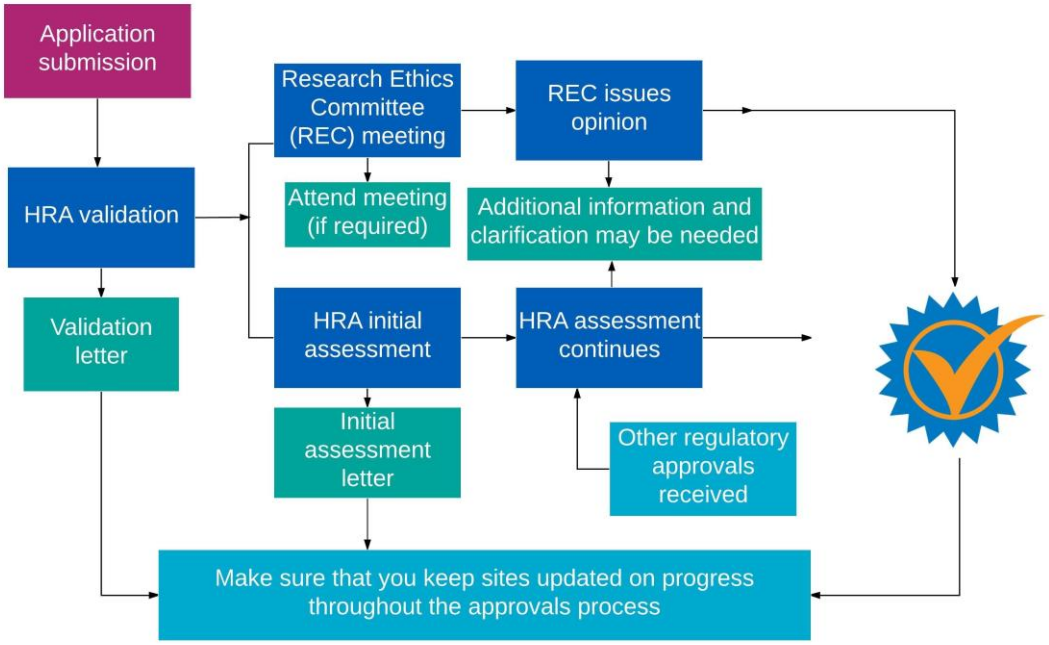


Figure 2: Diagram showing the main steps in gaining HRA Approval, from https://www.hra.nhs.uk/approvals-amendments/what-approvals-do-i-need/hra-approval/

[45] section 110(1)(d) of Care Act 2014

[46] *In Scotland section 251 approval can be sought from the Public Benefit and Privacy Panel for Health & Social Care (PBPP); and in N. Ireland advice can be sought from the HSC Privacy Advisory Committee.*

[47] http://www.dt-toolkit.ac.uk/routemaps/station.cfm?current_station_id=383

5.40. Where Section 251 approval is in place and the confidential information being disclosed would also be classified as personal data, the organisations holding this data (both the organisation disclosing the information and the recipient organisation) must also:

- have a lawful basis to hold and use personal data, and
- if applicable, have a condition to hold and use special categories of personal data, and
- be fair and transparent about how they hold and use this data.

Genuinely anonymised data will not require section 251 approval as disclosing it will not involve a breach of confidence.

5.41. Examples where section 251 consent has been granted include the Control of Patient Information Regulations 2002 (see below) which concern cancer registries which monitor mortality and survival rates.

Control of Patient Information Regulations 2002

5.42. The Health Service Control of Patient Information Regulations 2002 make provision for the processing of patient information, including confidential patient information for secondary purposes, without consent. They provide that patient information may be processed in accordance with these Regulations notwithstanding any common law obligation of confidence.

5.43. Regulation 2 makes provision relating to the processing of confidential patient information in connection with the construction and maintenance of databases by bodies (known as "cancer registries") which undertake the surveillance of health and disease of patients referred for the diagnosis or treatment of neoplasia[48]. Regulation 3 makes provision for the processing of confidential patient information for the recognition, control and prevention of communicable disease and other risks to public health.

5.44. Regulation 5 and the Schedule to the Regulations makes general provision in relation to the processing of patient information. Such processing is restricted to that approved by the Secretary of State and, in the case of processing for research purposes, the relevant ethics committee. The Schedule to these Regulations sets out the circumstances in which confidential patient information may be processed for medical purposes under regulation 5. The provisions relate, for example, to the processing of confidential patient information in order to identify who should be invited to participate in medical research (paragraph 3) or to enable the auditing, monitoring and analysing the provision made by the health service (paragraph 5).

5.45. Regulation 6 requires the Secretary of State to record and make public particulars relating to approvals which permit the transfer of confidential patient information. Regulation 7 restricts the processing of information under the Regulations, for example by requiring the removal of particulars by which the persons to whom information relates can be identified if that is practical.

[48] *The presence of formation of new, abnormal growth of tissue.*

Conclusions:

- For universities, NHS organisations or other public authority processing sensitive personal data for research without consent, the lawful bases for processing are most likely to be:
    - (Article 6(1)(e) of GDPR) 'necessary for the performance of a task in the public interest' or 'exercise of official authority vested in the controller'; and
    - (Article 9(2)(j) of GDPR) 'necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1)'.
- For private-sector or third-sector organisations, processing sensitive personal data for research without consent, the lawful bases for processing are most likely to be:
    - (Article 6(1)(f) of GDPR) 'necessary for the purposes of the legitimate interests except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data'; and
    - (Article 9(2)(j) of GDPR) 'necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1)'.
- Commercial interests cannot be the sole reason for relying upon these grounds and there must be some public interest pursued. Further guidance is required to confirm what will satisfy the 'public interest' test as many research projects will be commercially driven and the distinction between public interests and private gain becomes harder to identify.
- The general duty of confidence still applies, and patient records cannot be used (without consent) for research purposes where an individual has engaged the NHS opt-out; unless the HRA has granted specific authority for a research project to override the opt-out. The duty of confidence remains after death.

CAN PERSONAL DATA (PARTICULARLY BIOMETRIC DATA) EVER TRULY BE ANONYMISED / PSEUDONYMISED?

6.1. Anonymising data is the process of removing personal identifiers, both direct and indirect, that may lead to an individual being identified. Anonymised data falls outside the scope of GDPR (Article 26 of GDPR). However, organisations frequently refer to personal data sets as having been 'anonymised' when, in fact, this is not the case. To be truly anonymised under the GDPR, you must strip personal data of sufficient elements that mean the individual can no longer be identified. Organisations often refer to anonymisation when they more accurately describing pseudonymised data.

6.2. Pseudonymised data is the process of distinguishing individuals in a dataset by using a unique identifier which does not reveal their 'real world' identity. Even though pseudonymised data does not identify an individual, in the hands of those who do not have access to the 'key', the possibility of linking several anonymised datasets to the same individual can be a precursor to identification. Pseudonymised data (such as de-identified or de-personalised data, which can later be reconnected with the original identifying information), remains within the scope of GDPR.

6.3. The GDPR permits the processing of personal data where necessary for scientific research purposes if the appropriate safeguards are in place (Article 89 of GDPR). Those safeguard measures may include pseudonymisation provided the scientific research purposes can be fulfilled in that manner; but where anonymisation is possible, anonymisation must be used.

Anonymisation

6.4. There is growing concern that biometric and genetic data is inherently identifiable. As an identifier that is unique to each individual, it will almost always be possible to identify the natural person to which that biometric or genetic data belongs; regardless of the attempts to remove any other identifiers, labels or metadata attached to the biometric or genetic data.

It should first be considered if the processing can be done using anonymous data. If this is not possible then safeguards should be in place.

6.5. Even if true anonymisation is possible, it has been recognised that "fully anonymous data are more often than not, unsuitable for health research. The more intricate relations between exposure, the onset of disease, treatment regime and/or results of treatment can usually not be investigated with fully anonymous data."[49]

6.6. Whilst the researcher considering the information does not need to know who the person is, they do need to be assured that the data relates to one specific person and not to someone else, in order to acquire reliable data. Age group, gender, onset of disease, details about the disease, sometimes profession and location are often relevant research data and can in some circumstances be indirectly identifiable. If you could at any point use any reasonably available

[49] *'Patient data for health research: a discussion paper on anonymisation procedures for the use of patient data for health research' (Mr Evert-Ben Van Veen, October 2011)*

means to cross-reference and re-identify the individuals to which the data refers, that data will not have been effectively anonymised but will have merely been pseudonymised and remains personal data for the purposes of GDPR[50].

<table>
<tr><td>ANONYMOUS DATA</td><td colspan="2">Fully aggregated and/or anonymous data.</td></tr>
<tr><td rowspan="4">PERSONAL DATA</td><td colspan="2">Coded anonymous (pseudonymised data).</td></tr>
<tr><td rowspan="2">Indirectly identifiable data.</td><td>Coded but either coding insufficiently secure or aggregation level too low.</td></tr>
<tr><td>Not coded but aggregation level too low.</td></tr>
<tr><td colspan="2">Directly identifiable data.</td></tr>
</table>

Figure 3 *'Patient data for health research: a discussion paper on anonymisation procedures for the use of patient data for health research' (Mr Evert-Ben Van Veen, October 2011)*

Generally speaking, people within the healthcare system using data for secondary purposes must only use data that do not identify individual patients unless they have the consent of the patient themselves.[51]

6.7. Whilst it might be possible to remove the other personal data labels attached to the biometric and genetic data so that they are not directly or indirectly identifiable, by their very nature it will almost always be possible to trace the data back to an individual and to discern something about the person concerned.

6.8. A compliant approach can be more easily understood when considering the use of a trusted third party (**TTP**) to anonymise personal data held for use in a collaborative project. TTPs can be used to link datasets from separate organisations, and then convert the personal data into an anonymised form to create anonymised records for researchers. Whilst the organisations involved will not have access to each other's personal data, the ICO[52] highlights that other data (whether personal or not) can be linked to the anonymised data to result in re-identification. The ICO recognises that even complex statistical data, matched in a particular way, could result in re-identification[53] and steps must be taken to prevent a 'motivated intruder'.

[50] 'Patient data for health research: a discussion paper on anonymisation procedures for the use of patient data for health research' (Mr Evert-Ben Van Veen, October 2011)

[51] https://www.england.nhs.uk/ig/about/

[52] Page 41 onwards of the ICO's "Anonymisation: managing data protection risk code of practice " https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf

[53] *Please note it is a criminal offence to knowingly or recklessly to re-identify information that is de-identified personal data (section 171 of DPA 2018)*

6.9. The DPA does not require anonymisation to be completely risk free – you must be able to mitigate the risk of identification until it is remote. Clearly, 100% anonymisation is the most desirable position, and in some cases, this is possible, but it is not the test the DPA requires[54].

6.10. The published results of a study may well be anonymous, particularly where it has been irreversibly aggregated i.e. where statistical data about several individuals that has been combined to show general trends or values without identifying individuals within the data. Aggregated data is relatively low-risk, depending on granularity, and sample size.

6.11. Nevertheless, whilst steps can be taken to remove all existing labels, corresponding data or metadata, when it comes to the biometric and genetic data which forms the evidence of the study, organisations must consider that the passage of time, increase in resource and development of new technology may allow currently anonymised data to become identifiable at some point in the future.

Anonymisation may be possible on a temporary basis but it will almost always be possible to trace biometric and genetic data back to its source.

6.12. The key point is one of necessity and proportionality: the law will allow the use of identifiable data for medical research without consent, provided that such use is necessary and is proportionate with respect to privacy and public interest benefits. We understand that some hospitals are already communicating to their patients that DNA is unique and therefore it can never be completely anonymous. Due to the exemptions available in respect of scientific research and opportunities provided by pseudonymisation (discussed above), we consider the concept of 'anonymisation' does not require further analysis.

Pseudonymisation

6.13. If anonymisation is only a temporary safeguard at best, it is worth considering pseudonymisation (or key-coded data) as an alternative. Whilst pseudonymised data is a form of personal data, processing of pseudonymous data is actively encouraged under the GDPR and pseudonymisation is identified as a means of implementing appropriate safeguards to protect personal data. For example, Article 6(4) of the GDPR states that the pseudonymisation of data is a factor that controllers should consider when determining compatibility of purpose for further processing, and Article 25(1) includes pseudonymisation as an example of a measure which may satisfy requirements to implement data privacy by design.

6.14. The starting point in Article 89 of GDPR is to establish whether processing for scientific research purposes "can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner". In other words, it should first be considered if the processing can be done using anonymous data. If this is not possible then safeguards should be in place. These safeguards include:

- ensuring that technical and organisational measures are in place;
- ensuring that the principle of data minimisation (that is, the requirement to process only the minimum amount of personal data) is upheld.

[54] https://ico.org.uk/media/1061/anonymisation-code.pdf

6.15. Additional safeguards are included in section 19 of the DPA 2018 which require that:

- the data is not processed to support measures or decisions relating to particular individuals, unless this includes the purposes of approved medical research (which is defined in section 19);
- the data is not processed in such a way that substantial damage or substantial distress is likely to be caused to any data subject.

Conclusions:

- Anonymised data is only likely to be achieved in respect of aggregate data which cannot be dis-aggregated.
- Anonymised data is the default option where it is possible to carry out research using anonymised data.
- Pseudonymised data is an appropriate method for implementing suitable safeguards in compliance with GDPR.
- Other technical and security measures must still be considered to prevent any anonymisation or pseudonymisation steps being undermined by determined third parties.

HOW DOES THE HUMAN RIGHTS ACT IMPACT (OR ECHR) IMPACT THE USE OF PERSONAL DATA (IF APPLICABLE)?

7.1. Processing personal data, particularly for the purpose of carrying out medical research has resulted in significant public health benefits by identifying the causes and changing patterns of disease, improving therapeutic practice and the use of health care services, and by indicating promising areas of research. There are clear benefits to society to be gained from processing personal data lawfully, particularly where medical advances enable society to improve overall public health and to reduce health inequalities[55].

7.2. Nevertheless, we cannot yet identify all the consequences (whether beneficial or detrimental) arising out of processing personal data in a world which is building increasing reliance upon the inter-connectivity of goods and services in both our public and domestic environments. As a result, processing personal data also presents a potentially significant risk to individual welfare and there is growing pressure to take an approach to data governance which engages with international human rights[56].

"Data sharing is not, in human rights terms, objectionable in itself. But it inevitably raises human rights concerns… and the more sensitive the information, the stronger those concerns will be".[57]

7.3. The GDPR makes explicit reference to this approach and confirms that "restrictions concerning specific principles and the rights of information, access to and rectification or erasure of personal data, the right to data portability, the right to object, decisions based on profiling, as well as the communication of a personal data breach to a data subject and certain related obligations of the controllers … should be in accordance with the requirements set out in the Charter and in the European Convention for the Protection of Human Rights and Fundamental Freedoms" (Recital 73 of GDPR). In respect of data transfers, the GDPR explicitly states that "when assessing the adequate level of protection in respect of any data transfer, the Commission shall, in particular, take account of "respect for human rights and fundamental freedoms" (Article 45(2)(a)).

7.4. As the opportunities for processing data become more complex in a rapidly changing technological environment, data controllers will need to look beyond the historic focus on data quality and technical security and consider the impact of data processing on fundamental rights and collective social and ethical values.

---

[55] *The World Health Organisation recognises that "functioning national health information systems and availability of disaggregated data are essential to be able to identify the most vulnerable groups and diverse needs" -* https://www.who.int/news-room/fact-sheets/detail/human-rights-and-health

[56] *Human Rights are currently enforced in English law by virtue of the Human Rights Act 1998. Whilst this legislation may be subject to review over time, it is unlikely the principles enshrined within them will be removed.*

[57] Data Protection and Human Rights, House of Lords, House of Commons, Joint Committee on Human Rights, Fourteenth Report of Session 2007-08
https://publications.parliament.uk/pa/jt200708/jtselect/jtrights/72/72.pdf

Law of privacy

7.5. Privacy and Data Protection, though connected, are commonly recognised all over the world as separate rights. The House of Lords decided in Wainwright v Home Office [2003] 3 WLR 1137 that there was no general tort[58] of "invasion of privacy" in England and Wales. However, this does not mean that there is no law of privacy in England and Wales and indeed, a right to privacy has long been recognised and protected under English law in different guises, most recently as a result of the requirement to give effect to Article 8 of the Convention, through the application of the HRA 1998[59].

7.6. The key provisions of the Convention in relation to privacy are Articles 8 and 10. These provide that:

- everyone has the right to respect for his private and family life, his home and his correspondence. Public authorities may only interfere with the exercise of this right for various specific purposes insofar as is necessary in a democratic society, including the protection of the rights and freedoms of others. (Article 8 of HRA 1998)
- Everyone has the right to freedom of expression, the exercise of which may be subject to such restrictions as are prescribed by law and are necessary in a democratic society, for various purposes, including the protection of the reputation or rights of others and preventing the disclosure of information received in confidence. (Article 10 of HRA 1998)

7.7. The European Court of Human Rights has emphasised that "the protection of personal data, particularly medical data, is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life as guaranteed by Article 8 of the Convention. Respecting the confidentiality of health data is a vital principle in the legal systems of all the Contracting Parties to the Convention. It is crucial not only to respect the sense of privacy of a patient but also to preserve his or her confidence in the medical profession and in the health services in general." (*MS v Sweden* (1997) 28 EHRR 313, para 41).

7.8. It has long been established that the collection, storage, or disclosure of information relating to private life interferes with the right to privacy[60]. It has also been established that public information can become part of a person's private life where the records are "available for disclosure long after the event when everyone other than the person concerned is likely to have forgotten about it, [or the information concerns an event that occurred] in private"[61]. However, in the EU, privacy and data protection are not absolute rights and can be limited under certain conditions according to the Convention.

7.9. Whilst "the obligation to provide personal data, the release of personal data without consent, and the collection and storage of personal data all amount to interferences with an individual's

---

[58] *A civil wrong which causes a claimant to suffer loss or harm, resulting in legal liability for the person who commits a tortious act.*

[59] *The application of privacy law England and Wales will not be affected by the UK's referendum to withdraw from the EU (Brexit).*

[60] *Amann v Switzerland App* [2000] ECHR 88 and *R (on the application of Catt) v Association of Chief Police Officers of England, Wales and Northern Ireland* [2015] UKSC 9

[61] *M.M. v. THE UNITED KINGDOM (Application no. 24029/07)*

right to respect for his or her privacy"[62], "the rights to privacy and data protection may need to be balanced against other human rights, or public and private interests such as the fundamental rights to freedom of expression, freedom of the press or freedom of access to information [and] the rights to privacy and data protection may also need to be weighed up against other public interests, such as national security."[63] To be lawful, any interference with a person's Article 8 right to respect for private life:

- should be "in accordance with the law"; and
- proportionate to the objective; and
- necessary in a democratic society.

7.10. Whilst some may argue that the ability to detect cancer or diseases early will always outweigh the patient's desire to maintain the confidentiality of their patient records, legal action has challenged the release of medical records of deceased patients which were provided to the Redfern Inquiry into human tissue analysis - Lewis v Secretary of State for Health [2008] EWHC 2196 (QB). In this case, the Court held, the kind of examination that would have been conducted in order to obtain tissue would rank high in terms of intimacy and sensitivity, and the presumption would be that a high degree of confidentiality would endure for many years after the death of those concerned. Nevertheless, the public interest in disclosing the records outweighed the public interest in maintaining confidentiality of the same and accordingly the Court authorised disclosure to the Inquiry under its general powers.

7.11. The GDPR requires a controller to carry out a data protection impact assessment (DPIA) in advance of any processing which uses new technologies and is likely to result in a high risk for individuals (Article 35). Article 35(3) of the GDPR identifies three specific examples where a DPIA would be required. These include:

- where the evaluation of personal data about natural persons is based on automatic processing, including profiling.
- where special categories of personal data, such as health data, are being processed on a large scale (i.e. involving a wide range or large volume of personal data, taking place over a large geographical area, affecting a large number of people or having extensive and/or long-lasting effects).
- when systematically monitoring a publicly accessible area on a large scale.

7.12. This is part of the new focus on accountability and being able to demonstrate that you comply with the GDPR. DPIAs are designed to help identify and minimise the data protection risks of a project at an early stage. They can serve a dual purpose in evidencing that the controller has acted proportionately when undertaking any type of processing that is likely to result in a high risk as the controller must consider the impact on any of an individuals' rights and freedoms, including (but not limited to) privacy rights.

---

[62] Data Protection and Human Rights, House of Lords, House of Commons, Joint Committee on Human Rights, Fourteenth Report of Session 2007-08
https://publications.parliament.uk/pa/jt200708/jtselect/jtrights/72/72.pdf

[63] https://edps.europa.eu/data-protection/data-protection_en

Discrimination

7.13. The Equality Act 2010 prohibits direct and indirect discrimination by private companies in the provision of goods and services. Section 13 of the Equality Act 2010 prohibits direct discrimination, while Section 19 prohibits indirect discrimination (where a provision, criterion or practice puts people sharing a protected characteristic at a particular disadvantage, and this cannot be objectively justified). Private companies could be liable to breaching the prohibition on direct or indirect discrimination in relation to the way that they use technology - even if discrimination was not intended.

7.14. Bias in the data can create discriminatory outcomes and we have already referred to the bias created where consent is relied upon as the lawful basis for processing: too much onus on the individual to educate themselves on how the technology companies work rather than setting a high standard of protection by default. It can lead to data sets missing key information from sub-sets of individuals and placing an over-reliance upon the limited information which has been provided. Aside from human bias, algorithms can draw inferences from personal data, posing risks in terms of discrimination. In the context of 'big data' analytics, this can have a significant and long-lasting detrimental impact upon individuals even where the discrimination is unintended. Algorithms and automated processes can result in sophisticated trend analysis profiling, scoring systems and decision making which can impact essential services such as access to healthcare, insurance premiums and loan approvals to name a few.

7.15. The use of artificial intelligence does not guarantee that outputs will be free of human bias or discrimination[64] and the Joint Committee on Human Rights has recognised that "important decisions–such as whether to refuse someone access to a service–should never be made based on inferences from people's data"[65]. Great care must be taken to minimise decisions which can have a significant and/or long-term impact upon the health of individuals and the population as a whole.

7.16. Recognising that technologies can have considerable impact on people's lives, the GDPR introduces a new prohibition on automated decision-making and profiling "which produces legal effects" concerning the data subject (Article 22(1)) unless the type of automated decision-making is:

- necessary for the performance for the entry into or performance of a contract;
- authorised by union or Member State law; or
- based on the individual's explicit consent.

7.17. Organisations should be commended where they seek to involve individuals in the decisions made about their data, such as the Citizens' Biometrics Council and its work to "support a deeper understanding of public perspectives and values on biometrics"[66]. However, practical recommendations and best practice guidance are not enforceable unless put on a statutory footing and data controllers will be reliant upon case law (as it builds up over time) to determine how data governance intersects with human rights.

---

[64] https://ico.org.uk/about-the-ico/news-and-events/ai-blog-human-bias-and-discrimination-in-ai-systems/

[65] https://publications.parliament.uk/pa/jt201919/jtselect/jtrights/122/122.pdf

[66] https://www.adalovelaceinstitute.org/our-work/identities-liberties/citizens-biometrics-council/

7.18. Whilst the ICO adapts to the increasing demand on its resource, individuals will have very few avenues to enforce their rights, other than through the Courts. This is likely to result in organisations 'pushing the boundary' of human rights compliance until a breach occurs of such magnitude or severity that it generates a public interest case: sufficiently serious or impacting a significant number of individuals to justify a class action, that meaningful and swift corrective measures are taken to incentivise compliance.

Conclusions:

- The greatest risk that data processing poses to human rights is the unknown detriment that could be caused through unintended use of that data and the data-driven technologies that it results in.
- Current safeguards require the data subject to have a detailed knowledge of the risks and benefits but also the means to enforce their rights.
- Automated decision-making and profiling will require a Data Protection Impact Assessment.

WHAT IS THE IMPACT OF THE CURRENT FORM OF EU GDPR & DATA PROTECTION ACT 2018 ON DATA PROTECTION, HEALTH DATA AND LIFE SCIENCES?

8.1. The GDPR and new DPA brings enhanced protections for individuals and increased expectations of organisations processing personal data.

8.2. The definition of "personal data" is largely the same as pre-GDPR. We have already discussed above the additional safeguards afforded to the processing of biometric data and genetic data along with the legal grounds available for processing which have been included so as not impede research. The overarching principles remain the same in that organisations need to be lawful, fair and transparent when either controlling or processing personal data.

8.3. Key changes which have occurred as a result of GDPR include:

- a broad territorial reach applying to organisations established in the EU and to organisations established outside the EU where they carry out processing activities related to the offering of goods or services to individuals in the EU or the monitoring of individuals in the EU;
- if data is sent outside of the EU, data controllers need to demonstrate that controls and oversight are in place and the data is protected;
- data processors now have specific regulatory obligations (and liability) in relation to data protection;
- reduced time frame for dealing with subject access requests (without undue delay and at the latest within one month of receipt);
- for most life science organisations, the appointment of a Data Protection Officer is mandatory;
- a more aggressive enforcement approach with fines of up to 4% of a company's annual worldwide turnover or EUR 20 million, whichever is the greater;
- a greater awareness amongst the general public about their rights.

8.4. It is possible that the GDPR will lead to increased reliance on data protection legislation in privacy, discrimination cases and employment disputes, due to the strengthening of individuals' rights, the ability to request significant volumes of evidence (through a subject access request) and the hugely increased financial penalties that national regulators can levy for non-compliance with the provisions of the GDPR. This is dependent upon the ICO having sufficient resource to bring action against infringing organisations and it is still bringing enforcement under the old Data Protection Act 1998.

Conclusions:

- The GDPR has enhanced existing data requirements but has not radically changed the medical sector which already had a strong focus on confidentiality and patient autonomy.
- The overriding principles of fairness and transparency will remain key for all processing purposes.
- Commercial organisations which have a high tolerance of risk are likely to push the boundaries of compliance until enforcement action becomes a real and meaningful threat.

PART 3 - EXPLOITING INTANGIBLE PROPERTY

IS PERSONAL DATA AN INTELLECTUAL PROPERTY ASSET? CAN IT BECOME AN ASSET IF INCORPORATED INTO OTHER MATERIALS?

9.1. As a general principle, there is no property right in information itself: "there are no intellectual property rights in plain facts; these only arise when facts are arranged into databases."[67] While individual items of information do not attract property rights, original literary works, sound recordings, films and typographical arrangements may be protected by copyright and compilations of data may be protected by copyright and/or Database Right.

Databases: copyright and database right

9.2. A "database" means "a collection of independent works, data or other materials which are arranged in a systematic or methodical way and are individual accessible by electronic or other means" (section 3A(1) of the Copyright, Designs and Patents Act 1988 (**CDPA**).

9.3. Many compilations of data will fall within the statutory definition of a database, not least because there is no requirement for the database to be in electronic form. So, for example, a telephone directory is a database. There is however a distinction to be drawn between a database and its individual components.

Database right

9.4. If a data set falls within the definition of a database, and there has been "substantial investment in obtaining, verifying or presenting the contents of the database" it will qualify for protection in its own right under the Copyright and Rights in Databases Regulations 1997 (SI 1997/3032)[68].

Database right protects the collection of data, not its constituent elements.

9.5. Investment means "any investment, whether of financial, human or technical resources" and substantial means "substantial in terms of quantity or quality or a combination of both" (Regulation 13 of Database Regulations). Investment in actually creating data which forms part of a database will not automatically result in a database right. Organisations creating data must make separate investment in the organisation and arrangement of the database itself in order to gain the protection afforded by Database Right.

---

[67] Value of Data Bennett Institute – Policy implications, https://www.bennettinstitute.cam.ac.uk/media/uploads/files/Value_of_data_Policy_Implications_Report_26_Feb_ok4noWn.pdf

[68] *Which implemented the EU Database Directive (EU Directive 96/9/EC) in UK law.*

9.6. The maker of a database is defined as the person who "takes the initiative in obtaining, verifying or presenting the contents of a database and assumes the risk of investing in that obtaining, verification or presentation" and such person (provided they based in an EEA state) is the first owner of the Database Right (Regulation 14(1) of Database Regulations). An employer is regarded as the maker of a database made by an employee in the course of his employment, subject to any agreement to the contrary (Regulation 14(2) of Database Regulations).

9.7. A business which commissions a contractor to produce a database is likely to be the owner of the database right, since it would assume the risk of investing in the obtaining, verification or presentation of the contents of the database (whereas copyright in the database is likely to belong to the contractor as the author of the database – see below).

9.8. A Database Right is infringed if a person extracts or re-utilises all or a substantial part of the contents of the database without the owner's permission (Regulation 16(1) of Database Regulations) and therefore processing agreements must be carefully drafted to ensure that they address the ownership of any database right created by data processors. Extraction is defined in Regulation 12 as "the permanent or temporary transfer of all or a substantial part of the contents of a database to another medium by any means or in any form". Re-utilisation is defined as making the contents of a database available to the public by any means.

The circumstances in which a database might attract copyright protection are extremely limited, if available at all.

9.9. Database right exists independently of the copyright (if any) in a database and protects the compilation of information comprising the database. Database right lasts for **15 years** from the end of the calendar year in which the making of the database was completed (or, if the database is made available to the public before the end of this period, 15 years from the end of the calendar year in which the database was first made available to the public) (Regulation 17 of Database Regulations). This is a much shorter period of protection than that afforded by copyright, which lasts for 70 years from the end of the calendar year in which the author of the database dies.

9.10. A database which is protected by copyright therefore obtains a longer period of protection. However, if a "substantial change" to the contents of a database is made which would result in the database being considered to be a "substantial new investment", the amended database will qualify for a new 15-year term. In effect, this means that an indefinite term of protection is available for the many databases that are continually updated.

Copyright

9.11. Compilations of data that do not fall within the definition of a "database" under section 3A(1) of the CDPA (that is, a collection of independent works, data or other materials which are arranged in a systematic or methodical way and are individually accessible by electronic or other means) may nonetheless continue to be protected by copyright as literary works.

9.12. A database will only attract copyright protection if "the contents of the database the database constitutes the author's own intellectual creation" (section 3A(2) of CDPA). For example, an alphabetical list of traders within a particular area would in itself be unlikely to attract copyright protection (although it could qualify for the database right). However, if the traders were also graded for several other criteria by means of research carried out by the compiler of the database, including, for example, by reference to customer satisfaction, then it may attract copyright protection.

9.13. Copyright may also subsist in each work comprising part of a database. In the case of a database of photographs, for example, there may be copyright in the database itself and separate copyright in each photograph included in the database. However, it is important to remember that a key component of copyright is that the subject matter was the author's own intellectual creation

9.14. The first owner of copyright in a database will be the author of the database (that is, the person who creates it). In contrast to Database Right, this means that if a business commissions a contractor to create a database for it, the contractor is likely to be the first owner of copyright in the database. It is therefore important that, if a business has engaged a contractor to create a database for it, and wants to own copyright in that database, it enters into an agreement with the contractor which contains an assignment of copyright.

Copyright (along with all intellectual property rights) should be carefully considered and address in the terms of engaging any contractor to ensure that ownership and use rights are properly captured in the arrangement.

9.15. Generally, an employer is regarded as the copyright owner of a database made by an employee in the course of his employment, subject to any agreement to the contrary. Copyright in a database lasts for **70 years** from the end of the calendar year in which the author of the database dies. The law of copyright can only be used where it can be shown that a third party has copied the relevant work.

Examples of Copyright and Database Right in a data set

9.16. The UK Data Service is a national data service that provides research access to a range of social and economic data collections including UK census data and government funded surveys as well as qualitative and business data, funded by the Economic and Social Research Council. It includes on its website[69] some practical examples of copyright and Database Right in respect of public data and archiving.

9.17. The examples explain that where researchers analyse data sources which are subject to copyright they will need permission from the copyright holder before the data is copied and compiled into a new data set; employees and independent contractors own the copyright in their works by default, unless this has been addressed in their contract of engagement. Once researchers have analysed that data and created a new database, they may have Database Rights in the database they have created and copyright in the conclusions they draw, but the researchers cannot share those data sources unless they have permission to publish the original material.

9.18. It is also important to be aware that where data is held by the Crown, processing that data will give rise to jointly held copyright between the creator and the Crown.

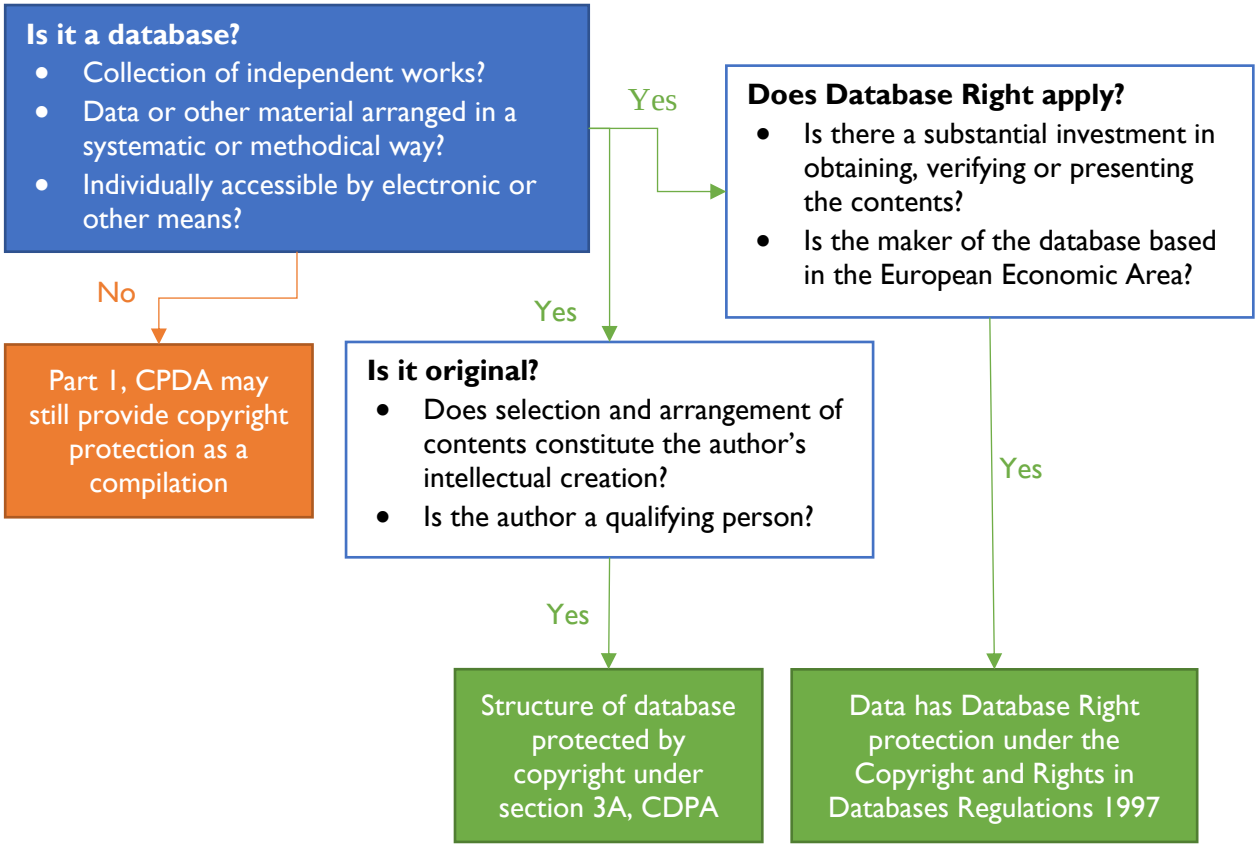
Alignment with data protection and consequences of 'Brexit'

9.19. Ownership of Database Rights or copyright does not necessarily give the owner unfettered rights to exploit the data contained in the database in all circumstances and they will still be expected to comply with data protection legislation. For example, where a database contains

[69] https://www.ukdataservice.ac.uk/manage-data/rights/scenarios.aspx

personal data, it cannot be shared where this would breach the GDPR or DPA e.g. contravening the individual's consent (if that was the lawful basis relied upon) or failing to implement adequate safeguards to protect the rights and freedoms of the data subject. This is one of the clear benefits in using pseudonymised data so that the results are only ever made available on a de-personalised or de-identified basis.

9.20. Under the UK-EU withdrawal agreement, Database Rights that subsist in the UK or EEA before the end of the transition period (whether held by UK or EEA persons or businesses) will continue to subsist in the UK and EEA for the rest of their duration. However, UK citizens, residents, and businesses will no longer be eligible to receive or hold new Database Rights in the EEA after the end of the transition period. UK legislation will be amended so that only UK citizens, residents, and businesses are eligible for new Database Rights in the UK after the end of the transition period. We will be considering the issue of international data transfers at a later stage.



Trade secrets

9.21. A trade secret is a specific form of confidential information which:

- is not, as a body or in the precise configuration and assembly of its components, generally known among, or readily accessible to, persons within the circles that normally deal with the kind of information in question;
- has commercial value because it is secret; and

- has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret commercial valuable, is treated as a secret and gives the owner a competitive advantage[70].

9.22. This can include formulae, recipes, algorithms and customer lists. The Trade Secrets Regulations 2018 do not replace the common law of confidentiality but are intended to operate in parallel with it. Recital 63 of GDPR confirms that the individual's right of direct access to their personal data "should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property".

9.23. When trying to find a balance between data protection rights and trade secret rights in customer information in the EU, it is clear that "customer data can be 'trade secrets' only if they are considered in their totality and in their complexity: it is obvious that single customer data (e.g. biographical information of one single client) are not valuable as trade secrets, and their disclosure does not adversely affect the intellectual work of the businesses."[71]

Patents

9.24. The patent system is intended to encourage inventors to publish details of inventions and how they are put into effect by providing inventors with a limited monopoly over their inventions so that, after the expiry of the patents protecting them, the inventions are available for the public to use freely. The choice of protection often lies between patenting and maintaining the innovation as a trade secret under the law of confidential information. In the UK, patents are subject to the Patents Act 1977 (**PA 1977**).

9.25. Patents are available for most industrially applicable processes and devices. They may cover: mechanical devices, methods for doing things, chemical compounds and mixtures of compounds. A patent is a negative right that permits the inventor to stop third parties from using the invention.

9.26. Patents are treated as personal property and can be assigned i.e. transfer ownership. The proprietor of a patent may also grant licences for all or some of the claims incorporated in the patent, on terms it chooses.

9.27. In contrast to the protection afforded by, for example, copyright or the law of confidential information, patent protection does not arise automatically and the filing of an application for a patent, followed by its grant, is necessary to obtain such protection. In the UK, as in many other countries, all legal interests in and transactions relating to patents must be registered. Patents have limited protection periods that require renewal at regular intervals to ensure continued subsistence.

9.28. A patent may only be granted for an invention if it is:

- new;
- involves an inventive step;
- capable of industrial application; and
- not specifically excluded from protection as a patent (section 1 of PA 1977).

---

[70] Regulation 2 of the Trade Secrets (Enforcement etc) Regulations 2018

[71] 'Trade Secrets v Personal Data: a possible solution for balancing rights', Gianclaudio Malgieri, International Data Privacy Law 2016, Vol 6, No2

9.29. In the UK an invention belongs to the employer if either:

- it was made in the course of the normal duties of the employee or in the course of specifically assigned duties falling outside his normal duties;
- it was made in the course of the duties of the employee and, because of the nature of the employee's duties and the particular responsibilities arising from them, the employee had a special obligation to further the interests of the employer's undertaking (section 39(1)(a) and (b) PA 1977).

9.30. A provision in an employment contract that inventions made outside the course of the employee's duties are to vest in the employer would be unenforceable (section 42, PA 1977).

9.31. Bodies that fund research, may stipulate as a condition of funding that ownership of inventions arising from the research will vest in them, or at least that they cannot be exploited without their consent. In the absence of express contractual provision to the contrary, the legal title to an invention made by an independent contractor will vest in the contractor, unless the court is prepared, on the facts, to imply a term into the contract giving ownership to the party that has commissioned the work[72].

It is important, therefore, before any such commissioned work is commenced, to agree in a written contract that all intellectual property rights in any invention arising out of the work will vest in the party that is paying for the work to be done.

9.32. In some circumstances, two or more parties may be jointly entitled to apply for a patent. Although there is some variation in the position internationally, the rule in the UK is that, in the absence of an agreement to the contrary between the joint applicants, one cannot assign or license its share of the patent without the consent of the other, although either can use the patent or exploit it without such consent (Section 36(2) of PA 1977).

Other intellectual property rights

9.33. Based on the understanding that health data will not be commissioned by individuals for private or domestic purposes and the data will not be released publicly or used for publicity purposes, we advise that moral rights (rights conferred on the creators of copyright works), defamation law (a claim that the photograph or film was tended to lower them in the estimation of right-thinking members of society generally) and similar image rights (an individual's proprietary right in their personality) will not be relevant to this project.

Conclusions:

- Mere ideas are not intellectual property rights. Copyright & the duty of confidentiality only become available once an idea has been developed to attract the necessary qualities outlined above or otherwise recorded to attract copyright.
- Data on its own is not an intellectual property asset but the arrangement of that data and conclusions drawn from that data may result in copyright, database right and trade secrets or the creation of inventions and other commercially sensitive information. Copyright exists in

[72] *Bio Pure Technology Ltd v Jarzon Plastics Ltd*, BL 0/087/05, 31 March 2005

recorded material, so where 'insights' take the form of written conclusions or papers, there is copyright in that written text. An individual might also have trade-secrets or know-how where they have drawn conclusions but have not yet recorded them.

- The processing of personal data by a third party may result in intellectual property rights which will be owned by the creator, whether that is an organisation or consultant, and may be capable of exploitation (subject to the rights of the data subject).

EXPLOITING PERSONAL DATA AS AN INTELLECTUAL PROPERTY ASSET

10.1. For a number of years, access to NHS data has been available for a fee, including information on all hospital admissions (**HES**) and on a significant proportion of primary care interactions (CPRD). These datasets have been available for decades to assist the advancement of health research[73]. Data is shared in anonymised format and according to well-structured processes governed by public agencies, such as NHS Digital, the Medicines and Healthcare products Regulatory Agency (**MHRA**) and the National Institute for Health.

10.2. In a world where big data has increasing value, the UK has "an opportunity to leverage its health data assets to benefit people in the UK and across the world – both through better health and through the generation of more research and development and economic growth."[74] As a consequence, when taking into account the increasing political pressures on funding health care, "failing to ensure that the NHS is properly compensated may imperil public trust in the medium- and long-term"[75].

10.3. There are powers within the NHS Act 2006[76] which enable CCGs and NHS trusts to do anything 'specified in section 7(2)(a), (b) and (e)-(h) of the Health and Medicines Act 1988 (provision of goods etc) for the purpose of making additional income available for improving the health services', subject to the limitation that the power may only be exercised to the extent that it 'does not to any significant extent interfere with the performance by the group of its functions'. This includes, at section 7(2)(f), the power "to develop and exploit ideas and exploit intellectual property". NHS bodies therefore the ability, albeit not an obligation, to exploit intellectual property on a commercial basis to generate income.

10.4. When considering the potential value of intangible assets and the investment opportunity they create, NHS bodies will also be conscious that they cannot fulfil their principal purposes unless "in each financial year, its total income from the provision of goods and services for the purposes of the health service in England is greater than its total income from the provision of goods and services for any other purposes."[77]

10.5. The value of any intellectual property and the income that can be generated through its exploitation will be driven by external factors such as the uniqueness of the data available, the investment required in order to turn it into something useful and the ability to commercialise any resulting products.

---

[73] https://digital.nhs.uk/data-and-information/data-tools-and-services/data-services/hospital-episode-statistics

[74] 'NHS data: Maximising its impact on the health and wealth of the United Kingdom' Saira Ghafur, Gianluca Fontana, Jack Halligan, James O'Shaughnessy & Ara Darzi

[75] NHS data: Maximising its impact on the health and wealth of the United Kingdom' Saira Ghafur, Gianluca Fontana, Jack Halligan, James O'Shaughnessy & Ara Darzi

[76] Sections 20 and 14Z5(1) of NHS Act 2006

[77] Section 43(2A) of NHS Act 2006

Licensing

10.6. Owners of intellectual property rights regularly exploit the value of their assets through licensing. Licences grant another person explicit permission to use the assets created by the rights holder, enabling the owner to recoup the cost of their initial investment and maintain the value of the asset for the future.

10.7. Licences can and frequently do contain clauses that limit what licensees can do with the data. By controlling the use of intellectual property assets, for commercial purposes or otherwise, the author can maintain the value of the asset (as a limited resource) and protect the licensor from losing revenue by stopping the licensees from making the data available to third parties other than on commercial terms which favour the owner. Whilst some have asserted that "data cannot be shared for purely profit-making reasons"[78], this restriction only applies to information disseminated by the HSCIC (i.e. NHS Digital) which must ensure that information is only disseminated if it supports the provision of health and social care or the promotion of health[79] (although note above the different powers available to CCGS and NHS trusts above at paragraph 10.3).

10.8. Alternatively, the intellectual property owner may consider dedicating the data to the public domain, which means waiving intellectual property rights in the asset[80]. We have included below, by way of illustration, a table of possible value-sharing frameworks, produced as part of Imperial College's white paper on maximising the potential value of NHS data.

[78] https://www.kingsfund.org.uk/publications/using-data-nhs-gdpr

[79] Section 261(1A) Health and Social Care Act 2012

[80] Bennett Institute for Public Policy – the value of data https://www.bennettinstitute.cam.ac.uk/media/uploads/files/Value_of_data_Policy_Implications_Report_26_Feb_ok4noWn.pdf

*Value-sharing framework for the NHS, produced by '**NHS data: Maximising its impact on the health and wealth of the United Kingdom**' (2020) Saira Ghafur, Gianluca Fontana, Jack Halligan, James O'Shaughnessy & Ara Darzi*

AGREEMENT	DESCRIPTION	MAIN BENEFITS FOR THE NHS	POTENTIAL ISSUES
NO VALUE SHARING	The NHS shares data for free.	No direct economic benefit for NHS, but there is potential for patient and system wide benefit by openly sharing data for free.	• The NHS does not get any share of the economic return on products using the data or access to products.
FREE OR DISCOUNTED PRODUCTS	The product developed using an NHS dataset is provided to the contributing NHS organisation for free or at a discount (for a defined or unlimited period of time.) The product might also be offered to the rest of the NHS at a discount.	NHS as a whole or an individual organisation gets access to cutting-edge products at no or reduced cost.	No additional value specifically captured from product revenues. • Risk that no useful product is developed. • If the product is discounted or free only for one organisation, other NHS organisations will still have to pay for it. • The provision of a product free of charge would need to be reviewed to ensure no breach of regulatory compliance obligations by industry.
ONE-OFF PAYMENT	NHS receives a one-off payment in exchange for access to the data.	• Quick and certain access to funds with no risk or ongoing relationship required. • Potential to license same datasets for same uses to multiple parties to maximise revenue.	Depending on the pricing, this could generate limited value for the NHS (e.g., HES). • Depending on the fee, this may create a financial barrier to initial access to data, potentially penalising smaller companies.
ROYALTY/REVENUE SHARE	The NHS receives a royalty on revenue from products developed using its data.	• Potential long-term source of income. • Likely to generate the most income for the NHS.	• NHS would have to pay for tools developed using its data. • Risk that no revenue-generating product is developed. • Industry may require exclusivity in respect of the data limiting the NHS's ability to deal in the data with third parties.

*Value-sharing framework for the NHS, produced by '**NHS data: Maximising its impact on the health and wealth of the United Kingdom**' (2020) Saira Ghafur, Gianluca Fontana, Jack Halligan, James O'Shaughnessy & Ara Darzi*

AGREEMENT	DESCRIPTION	MAIN BENEFITS FOR THE NHS	POTENTIAL ISSUES
PROFIT SHARE	The NHS receives a portion of the profits generated by its industry partner.	NHS receives income every year that the company is profitable (irrespective of whether a specific profitable product is created).	NHS would have to pay for tools developed using its data. • May be resisted by established partners and therefore adopted by small and medium-sized enterprise (SME) partners which may not be profitable for some time. • Industry may require exclusivity in respect of the data limiting the NHS's ability to deal in the data with third parties.
IP OWNERSHIP SHARE	The NHS owns (alone or jointly) some of the intellectual property generated in the project which uses its data.	IP ownership for the NHS. • Potential for royalties based on the use of the NHS-owned IP as part of a wider package. • Potential to have some control over how the IP is used and exploited (subject to contractual arrangements).	• IP ownership does not itself generate revenue. • Difficult to manage: will tie NHS into a relationship with the company for as long as it retains a joint ownership interest, creating an administrative burden for the NHS. • Unappealing to companies: NHS involvement might complicate decision making and hinder company progress. • Unusual for mere provision of data to justify IP ownership; the NHS will likely need to demonstrate a more substantial role in the co-development of any IP e.g. clinical input. • Industry may require exclusivity in respect of the data limiting the NHS's ability to deal
EQUITY SHARE	The NHS receives a share of the equity of the company developing solutions from the data.	Ownership interest in company developing product and potential to have a say in its activities.	Difficult to decide what a fair share of the equity for the NHS would be. • Main return might be capital appreciation on sale (if any) as little or no dividends might be generated for a while.

*Value-sharing framework for the NHS, produced by '**NHS data: Maximising its impact on the health and wealth of the United Kingdom**' (2020) Saira Ghafur, Gianluca Fontana, Jack Halligan, James O'Shaughnessy & Ara Darzi*

AGREEMENT	DESCRIPTION	MAIN BENEFITS FOR THE NHS	POTENTIAL ISSUES
			• Likely unappealing to established companies. • NHS involvement as a minority shareholder might complicate company decision making and be burdensome to manage for the NHS. • Industry may require exclusivity in respect of the data limiting the NHS's ability to deal in the data with third parties.
GOLDEN SHARE	The NHS receives an equity share which is able to outvote all other shareholders in certain predetermined circumstances.	NHS or DH could essentially control the business and therefore require the company to be based in the UK and provide ongoing benefits to the health system.	• Restrictive model for industry, giving the NHS or the Government control over strategic decisions. • Unclear financial benefit for the NHS; this would result from the direction of the management of the company. • This model seems unlikely to be used where the only contribution is data. Rather this (and ownership of IP above) suggests a more integrated development team (e.g., NHS provides clinical test bed, clinical expertise and a strong package of rights in return for industry). • Industry may require exclusivity in respect of the data limiting the NHS's ability to deal in the data with third parties.
MULTIPLE ONE-OFF FEES LINKED TO PRODUCT SALES	NHS receives multiple one-off payments triggered by the licensee achieving certain regulatory and product milestones (e.g., start of clinical trial, regulatory approval,	Increased revenue vs one-off payment. • Less complex to administer vs other models.	If product is unsuccessful NHS may only receive small sum. • Audit may be required to verify if milestones have been met.

*Value-sharing framework for the NHS, produced by '**NHS data: Maximising its impact on the health and wealth of the United Kingdom**' (2020) Saira Ghafur, Gianluca Fontana, Jack Halligan, James O'Shaughnessy & Ara Darzi*

AGREEMENT	DESCRIPTION	MAIN BENEFITS FOR THE NHS	POTENTIAL ISSUES
	volume of sales, in each case of a product relying on the relevant data).	• More likely to be accepted by industry as payments linked to success. • Could reduce the "financial barrier" for smaller companies as mentioned above as larger payments are made when/if a product is successful.	• Total milestone payments may only be a fraction of overall revenues if product is highly successful.
SPIN-OUT	DH sets up a wholly owned business to hold the relevant IP or data asset with a view to obtaining further investment in the company or out-licensing.	Would allow DH to ringfence legally, financially and operationally key assets for commercialisation.	Until a third-party investor or collaborator is engaged, this vehicle would not generate any revenue. • Might be perceived by the public as a wholesale effort to commercialise data.

10.9. As part of its analysis in preparing the above table, Imperial's Institute for Global Health Innovation has recognised that "estimating the value of and potential benefits from the data is very difficult, which makes the development of robust business cases and the negotiation of fair value sharing agreements a big challenge."[81] One option not analysed above is the potential for developing a Sovereign Health Fund which would seek to guarantee the 'fair distribution' of associated benefits. This could be achieved through a fund which invests in a portfolio of healthcare assets and enterprises to generate a long-term return, where proceeds are ring-fences for health and care in the UK and afford citizens a say and a stake in how those proceeds were deployed.

10.10. Even if a 'fair' or 'market' value can be attributed to a piece of data or data set it is often still difficult to determine who exactly used the data-collecting device, and therefore who generated the data and would be entitled to the royalty. Where this is achievable, it will arguably be so administratively expensive that it could negate all value added by the data processing.

A data subject royalty paid to individuals is not practical where data is anonymised and/or aggregated so that it is not possible to discern the origin of the data.

10.11. Furthermore, "exclusive access to data should not be granted where data has been assembled by the NHS or another government-funded organisation. Granting exclusivity is unlikely to be in the public interest or the interest of science and the Department of Health & Social Care has recently banned NHS Trusts from striking exclusivity deals with the private sector."[82] This is addressed explicitly in the DHSC's 'Code of conduct for data-driven health and care technology' which states " careful consideration should be given before granting exclusivity of access to data, as exclusivity can limit benefit to the health and care system."[83] This also reflects the principles outlined in the Re-use of Public Sector Information Regulations 2015.

Public Sector Information (PSI)

10.12. The public sector collects, processes and disseminates huge quantities of information as a result of the exercise of its public functions, including information about finance, business, law, geography, traffic and tourist information. Businesses and individuals can benefit from provision of, and access to, this type of information and the opportunity to use it for their own purposes. This is particularly true with developments in information technology, which have led to unprecedented possibilities to combine data from different sources and create new products and services to exploit.

---

[81] NHS data: Maximising its impact on the health and wealth of the United Kingdom' Saira Ghafur, Gianluca Fontana, Jack Halligan, James O'Shaughnessy & Ara Darzi

[82] NHS data: Maximising its impact on the health and wealth of the United Kingdom' Saira Ghafur, Gianluca Fontana, Jack Halligan, James O'Shaughnessy & Ara Darzi

[83] https://www.gov.uk/government/publications/code-of-conduct-for-data-driven-health-and-care-technology/initial-code-of-conduct-for-data-driven-health-and-care-technology

The Re-use of Public Sector Information Regulations 2015 are intended to encourage re-use of public sector information and to ensure that any conditions imposed upon the re-use of public sector documents are fair, proportionate and non-discriminatory.

10.13. Any information (content) whatever its medium (form) – including print, digital or electronic, and sound recordings – produced, held or disseminated by a public-sector body in carrying out its public functions, is considered public sector information. If a public-sector body holds the copyright for information it produces, holds or disseminates within its public task, then that information is within the scope of the Re-use of Public Sector Information Regulations 2015.

Information generated by a public body in the course of delivering on its public task – is held by the Crown and should be licenced using the Open Government Licence, free of charge.

10.1. The Re-use of Public Sector Information Regulations 2015 constrains the ways in which public sector information can be licensed, ensuring that no exclusive licences are granted (which would prevent the public body from granting a licence to other re-users) and ensuring no one is given preferential terms. It was hoped that better use of public documents would lead to other public benefits, in the form of a range of added-value information products that the public sector itself could not provide, which would contribute to economic growth and other benefits. However, it remains the case that many public bodies are resistant to share information, particularly that which they consider to be commercially sensitive, whether under the Re-use of Public Sector Information Regulations 2015 or the Freedom of Information Act 2000.

10.2. If a public-sector body carries out research activities (capturing most public-sector bodies) it and the resulting research information are in scope. Where the regime applies, the public-sector body is obliged to permit re-use of a document on request under Regulations 6 and 7(1) and should make information and related metadata available through standard licences[84] (Regulation 11). For the purpose of these Regulations, "document" means any information recorded in any form, including any part of such information, whether in writing or stored in electronic form or as a sound, visual or audio-visual recording, other than a computer program."

10.3. Re-use means using public sector information, for a purpose other than the initial public task it was produced for. Typically, this would mean an individual, a company or other organisation taking information you have produced and republishing it or using it to produce a new product or resource, often by combining it with other information. This is sometimes, though not always, on a commercial basis.

10.4. A public-sector body may impose conditions on the re-use of its public-sector information, provided that those conditions do not:

- unnecessarily restrict competition or the way in which a document can be re-used (regulation 12(2)).

[84] *The Open Government Licence (OGL)*

- discriminate between applicants who make a request for re-use for comparable purposes (including use by the public sector for activities which fall outside the scope of its public task).

10.5. Any public-sector body that is subject to the 2015 Regulations may charge for allowing re-use of public-sector information (Regulation 15). However, any charges imposed by the public-sector body must be limited to the marginal costs incurred in respect of the reproduction, provision and dissemination of document. For example, NHS Digital, the central repository of NHS information, is not allowed to sell data for profit but operates on a cost recovery basis. It is allowed to charge for the cost of processing and delivering the service, but not for data itself. The charge depends on the type of application, amount of data requested, and the amount of work that NHS Digital will need to do"[85].

10.6. Despite the above, it is possible to charge higher than marginal costs in circumstances under Regulation 15(3)-(4) where:

- a public-sector body is required to generate revenue to cover a substantial part of the costs of fulfilling its public task (for example the CQC is required to generate income through its registration fees and issuing fines to providers carrying out regulated activities); or
- the public-sector body is required (by law, binding rules or common administrative practice) to generate revenue to cover a substantial part of the cost of their collection, production, reproduction or dissemination.

10.7. Any charges above marginal costs must not exceed the sum of direct costs, a reasonable apportionment of indirect and overhead costs attributable to chargeable activity, and a reasonable return on investment (Regulation 15(6)).

10.8. It is important to note that educational and research establishments including organisations established for the transfer of research results (such as research councils, schools and universities) fall outside the scope of the 2015 Regulations (Regulation 5(3)). The 2015 Regulations also do not apply where:

- the activity of supplying the document is one that falls outside the public-sector body's public task (regulation 5(1)(a));
- a third party owns relevant intellectual property rights in the document (Regulation 5(1)(b));
- access to the document is excluded or restricted under information access legislation, including on grounds of protection of personal data[86] or commercial confidentiality, amongst others. This includes information, therefore, that would attract the protection of an exemption or an exception under FOIA and the EIR (Regulation 5(7)(a)); or
- it is accessible under information access legislation and contains personal data, the re-use of which would be incompatible with data protection law (Regulation 5(7)(b)(ii)).

---

[85] https://understandingpatientdata.org.uk/what-you-need-know

[86] *Official guidance on the interplay between the Regulations and EU data protection laws pre-dates the GDPR and has yet to be fully updated.*

10.9. Where a public-sector body does decide to make public sector information available (that is also personal data), it must ensure that the relevant personal data is anonymised, or that it is made available under conditions that ensure the adequate protection of personal data such as pseudonymisation.

Conflicts of interest

10.10. We have outlined above (at section 9) the issues arising where the NHS enters into arrangements with third parties and independent contractors who may create and subsequently own intellectual property through their engagement with the NHS. Contracts must carefully consider and address the value of newly created materials and how this is apportioned between the parties. For example, CCGs are required to "make arrangements for managing conflicts and potential conflicts of interest in such a way as to ensure that they do not, and do not appear to, affect the integrity of the group's decision-making processes" (Section 14O of the NHS Act 2006).

10.11. It is important to remember that when commissioning third parties to deliver services, the Public Contracts Regulations 2015 (PCR 2015) applies to all contracts for NHS and non-NHS healthcare services with a total value of EUR750,000 or more, unless an exclusion applies. As of 1 January 2020, the corresponding value in GBP is 663,540[87]. This means that 'best value' and the avoidance of conflicts must be considered at the point of selecting a suitable partner, long before any intangible assets have been created.

10.12. NHS England's Managing conflicts of interest: revised statutory guidance[88] makes passing reference to the potential issues created by the creation of patents but does not offer substantive guidance on how this should be managed in practice. There is a gap in the legislation and statutory guidance which obliges NHS bodies to not undervalue data but also permits NHS bodies wide discretion when determining the value that can be achieved. Until standard practice is introduced, the value of health data and the cost / benefit analysis of exploiting it will need to be considered on a case-by-case basis.

Move to a standardised process

10.13. In order to eliminate delays caused by contract negotiations and legal reviews for each NHS site, the National Institute for Health Research (**NIHR**) has developed a new, standardised, national approach to costing and contracting for commercial contract research which are intended to "speed up the contracting process for industry-sponsored trials carried out in the NHS by removing the need for site-by-site reviews and local legal agreements to be drawn up"[89]. For example, there is a model Industry Collaborative Research Agreement which aims to support clinical research collaborations involving the pharmaceutical and biotechnology industries, academia and NHS organisations across the UK. However, these

---

[87] The National Health Service (Procurement, Patient Choice and Competition) Regulations 2013 require the NHS to achieve "best value for money" when procuring health care services (all forms of health care provided for individuals, whether relating to physical or mental health), but this does not extend to purchasing health-related services (services that may have an effect on people's health but are not health care services or social care services) – Health and Social Care Act 2012 sections 62 and 64.

[88] https://www.england.nhs.uk/publication/managing-conflicts-of-interest-in-the-nhs-guidance-for-staff-and-organisations/

[89] https://www.nihr.ac.uk/documents/model-site-agreements-model-contracts-standard-research-agreements/11612

model contract templates are only suitable in narrowly defined circumstances and their use is in no sense mandatory for companies, universities or NHS organisations.

Conclusions:

- Individuals do not 'own' their personal data but have rights which restrict how their data may be processed by others.
- Public bodies which generate information through carrying out a public task are obliged to make that data available to others on fair terms, ensuring charges are proportionate and prohibited from granting exclusive rights.
- The market will determine the 'fair value', 'market value' or 'best value' of any data. The difficulty in the health sector is that the market comprises commercial, not-for-profit and public bodies which may consider the data extremely 'valuable' but for reasons other than generating a monetary profit.
- The purpose and means of ensuring individuals receive a 'fair share' of the income generated by their personal data is still largely a philosophical issue and will be open to exploitation by commercial organisations until political pressures demand otherwise.
- Potential models for realising a 'data dividend' include: a royalty right in personal data (a licenced based fee enforced by representative bodies or a central institution) or a system of central collection and distribution of a fair share (through taxation or payment into a central fund).

WHAT REQUIREMENTS MUST BE MET FOR SHARING / SELLING PERSONAL DATA BY AN NHS BODY TO ANOTHER ORGANISATION WITHIN THE UK?

11.1. The legal framework governing the use of personal confidential data in health care is complex. It includes the NHS Act 2006, the Health and Social Care Act 2012, the Data Protection Act, and the Human Rights Act.

Information Standards and processing information

11.2. Information Standards (including data collections and extractions) are an agreed set of rules, a consistent method or process for capturing, processing, managing and sharing data and information.

11.3. Any registered person (a manager or service provider in respect of a regulated activity) who carries on an activity which involves, or is connected with, the provision of health care **must** have regard to any guidance published by NHS England in relation to the processing of patient information and any other information obtained or generated in the course of the provision of the health service[90]. These include Information Standards. Within the NHS and the wider health and social care system the term Information Standards also cover the specifications used to collect and extract data from information technology systems.

11.4. The full list of current information standards and collections is available on the NHS Digital website[91]. The list is updated on a monthly basis, following the approval of new items, and changes, by the data coordination board. Each standard includes guidance on how it should be implemented.

11.5. Whilst the standards do not currently apply to the private healthcare sector, under the changes proposed in the Acute Data Alignment Programme (**ADAPt**), NHS Digital and the Private Healthcare Information Network (**PHIN**) have launched a programme which aims to bring about an alignment in data standards, measurement and reporting systems across NHS and private healthcare in order to enable greater transparency in quality and safety, support patient choice, and provide opportunities for improving patient care[92].

NHS Digital / Health & Social Care Information Centre

11.6. From July 2016, the Health and Social Care Information Centre (**HSCIC**)[93] changed its name to NHS Digital. HSCIC, now NHS Digital, is the guardian of patient data and provides a range of guidance on data security and information governance to assist health and care organisations meet the standards required to handle people's health and care information[94].

---

[90] section 13S of National Health Service Act 2006.

[91] https://digital.nhs.uk/data-and-information/information-standards/information-standards-and-data-collections-including-extractions/publications-and-notifications/standards-and-collections

[92] https://digital.nhs.uk/news-and-events/latest-news/nhs-digital-and-phin-launch-consultation-on-next-phase-of-acute-data-alignment-programme

[93] Established by section 252 of the H&SC Act 2012.

[94] https://digital.nhs.uk/

NHS Digital does not however, enforce industry standards in relation to the permitted uses of patient data or its potential exploitation. Whilst NHSX is looking to step into this role, any guidance issued by it currently lacks the statutory status required to drive meaningful change.

11.7. The HSCIC has published a code of practice[95] on the actions to be taken in relation to the collection, analysis, publication or other dissemination of confidential information concerning or connected with the provision of health services or of adult social care in England. The code of practice describes good practice for organisations handling confidential information concerning, or connected with, the provision of health services or adult social care and applies to:

- health or social care bodies that collect, analyse, publish or otherwise disseminate confidential information concerning, or connected with, the provision of health services or of adult social care in England, and
- persons other than public bodies who provide health services or adult social care in England pursuant to arrangements made with a public body exercising functions in connection with the provision of such services or care.

11.8. Where an organisation meets these criteria then it **must** have regard to the code of practice[96]. Individuals and organisations may receive confidential information through a data sharing agreement requiring them to have regard to the code of practice. In such a case they **must** have regard to the code of practice[97].

UK policy framework for health and social care research

11.9. The Health and Research Authority (**HRA**) is the body responsible for the co-ordination and standardisation of practice relating to the regulation of health and social care research and functions relating to approvals for processing confidential information relating to patients[98].

11.10. The UK policy framework for health and social care research[99] sets out principles of good practice in the management and conduct of health and social care research that take account of legal requirements and other standards. This policy framework applies to health and social care research[100] that is within the responsibility of the HRA or the Devolved Administrations' Health Departments (see appendix 1). This includes:

- research concerned with the protection and promotion of public health;

---

[95] HSCIC 'Code of practice on confidential information' https://digital.nhs.uk/binaries/content/assets/legacy/pdf/8/9/copconfidentialinformation.pdf

[96] Section 263(6) H&SC Act 2012

[97] Section 263(7) H&SC Act 2012

[98] Section 110 Social Care Act 2014

[99] https://www.hra.nhs.uk/planning-and-improving-research/policies-standards-legislation/uk-policy-framework-health-social-care-research/

[100] Any research into matters relating to people's physical or mental health (section 110(3) Care Act 2014).

- research undertaken in or by a UK Health Department, its non-Departmental public bodies or the NHS and regulated social care providers (this does not appear to extend to all bodies that will have access to health or social care records); and
- clinical and non-clinical research, undertaken by NHS or social care staff using the resources of health and social care providers and any research undertaken within the health and social care systems that might have an impact on the quality of those services.

11.11. In accordance with Section 111(6) and (7) of the Care Act 2014, the status of the UK policy framework is statutory guidance to which local authorities, NHS trusts and NHS foundation trusts in England must have regard. Compliance with this guidance by them and other health and social care providers (such as independent contractors in primary care and private and voluntary organisations providing services under contract) also helps bodies that commission care to fulfil their legal duty under the Health and Social Care Act 2012 to promote the conduct of research.

11.12. The policy framework outlines the following principles that apply to all health and social care research:

- The **safety** and well-being of the individual prevail over the interests of science and society;
- All the people involved in managing and conducting a research project are qualified by education, training and experience, or otherwise **competent** under the supervision of a suitably qualified person, to perform their tasks;
- Research projects are **scientifically sound** and guided by **ethical** principles in all their aspects;
- **Patients, service users and the public are involved** in the design, management, conduct and dissemination of research, unless otherwise justified;
- Research is designed, reviewed, managed and undertaken in a way that ensures **integrity, quality and transparency**;
- The design and procedure of the research are clearly described and justified in a research proposal or **protocol**, where applicable conforming to a standard template and/or specified contents;
- The researchers and sponsor familiarise themselves with relevant **legislation** and guidance in respect of managing and conducting the research;
- Before the research project is started, any anticipated **benefit for the individual** participant and other present and future recipients of the health or social care in question is weighed against the **foreseeable risks** and inconveniences once they have been mitigated;
- A research project is started only if a research ethics committee and any other relevant **approval** body have favourably reviewed the research proposal or protocol and related information, where their review is expected or required;
- In order to avoid waste, information about research projects (other than those for educational purposes) is made **publicly available** before they start (unless a deferral is agreed by or on behalf of the research ethics committee);

- Other than research for educational purposes and early phase trials, the findings, whether positive or negative, are made **accessible**, with adequate consent and privacy safeguards, in a timely manner after they have finished, in compliance with any applicable regulatory standards, i.e. legal requirements or expectations of regulators. In addition, where appropriate, information about the findings of the research is available, in a suitable format and timely manner, to those who took part in it, unless otherwise justified;
- Research participants are afforded respect and autonomy, taking account of their capacity to understand. Where there is a difference between the research and the standard practice that they might otherwise experience, research participants are given information to understand the distinction and make a **choice**, unless a research ethics committee agrees otherwise. Where participants' explicit consent is sought, it is voluntary and informed. Where consent is refused or withdrawn, this is done without reprisal;
- Adequate provision is made for **insurance** or indemnity to cover liabilities which may arise in relation to the design, management and conduct of the research project.
- All information collected for or as part of the research project is recorded, handled and stored appropriately and in such a way and for such time that it can be accurately reported, interpreted and verified, while the **confidentiality** of individual research participants remains appropriately protected. Data and tissue collections are managed in a transparent way that demonstrates commitment to their appropriate use for research and appropriate protection of privacy.
- **Sanctions** for non-compliance with these principles may include appropriate and proportionate administrative, contractual or legal measures by funders, employers, relevant professional and statutory regulators, and other bodies.

11.13. At an individual level, the Court has confirmed in *Lloyd v Google LLC* [2019] EWCA Civ 1599 "a person's control over data… does have a value, so that the loss of that control must also have a value" but recognised that 'damage' is limited to non-financial loss, such as distress[101] and there does not, therefore appear to be a right for individuals to sue where their data is sold for an undervalue: their legal action remains limited to making a claim for damages where they have suffered a 'loss of control' over their data.

NHS Constitution and the legal duty to 'have regard to'

11.14. The NHS Constitution establishes the principles and values of the NHS in England. It sets out rights to which patients, public and staff are entitled, and pledges which the NHS is committed to achieve, together with responsibilities, which the public, patients and staff owe to one another to ensure that the NHS operates fairly and effectively[102].

[101] Section 169(5) of DPA 2018

[102] The NHS Constitution – the NHS belongs to us all (2015) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/480482/NHS_Constitution_WEB.pdf

11.15. Section 2 of the Health Act 2009 creates a duty for a defined list of NHS bodies and providers of NHS services[103] to "have regard" to the Constitution. As well as the NHS bodies listed in section 2(2) of the Health Act 2009, any person (for example a private provider or voluntary organisation) who provides health services under a contract, agreement or other arrangement, or any person who makes arrangements under a sub-contract for another person to provide or assist in providing those services, or any person who is providing or assisting in providing health services under a sub-contract, must also have regard to the NHS Constitution[104]. The duty is therefore far-reaching and applies to any provider who holds a contract with an NHS commissioner or who operates as a sub-contractor to an NHS provider.[105]

11.16. The Constitution includes seven key principles that guide the NHS in all it does:

- The NHS provides a comprehensive service, available to all;
- Access to NHS services is **based on clinical need, not an individual's ability to pay**;
- The NHS aspires to the highest standards of excellence and professionalism;
- **The patient will be at the heart of everything the NHS does**;
- The NHS works across organisational boundaries and in partnership with other organisations in the interest of patients, local communities and the wider population;
- The NHS is committed to providing **best value for taxpayers' money** and **the most effective, fair and sustainable use of finite resources**;
- The NHS is accountable to the public, communities and patients that it serves.

11.17. What is lacking is a definition of 'best value' or a practical means by which it can be calculated. This is probably because 'best value' will depend on so many individual factors, at most what could be achieved over some guidelines which still grant NHS bodies a broad discretion as to how they reach their conclusions. This is problematic in that it will create inconsistencies throughout the organisation and amongst the expectation of independent parties who come to collaborate with the NHS.

11.18. Whilst it may not be possible to directly enforce the Constitution, the duty to 'have regard' to the NHS Constitution is a legal duty[106] to consider the patient 'rights' created by the NHS Constitution when exercising functions. In order to take a lawful decision to depart from the NHS Constitution, an NHS body would have to have very carefully considered the relevant provisions of the NHS Constitution and to have departed from it for good reasons.

---

[103] *The bodies are: National Health Service trusts, the National Health Service Commissioning Board, clinical commissioning groups, local authorities, Special Health Authorities, the National Institute for Health and Care Excellence, the Health and Social Care information Centre, NHS foundation trusts, Monitor, the Care Quality Commission, Health Education England.*

[104] section 13S of H&SC Act 2012

[105] 'NHS Law and Practice', David lock QC and Hannah Gibbs

[106] Section 2 of the Health Act 2009.

11.19. Put broadly, decision-makers should ensure that their decision-making process, including a consideration of the relevant part of the Constitution and any reasons for acting in a way contrary to the Constitution, is clearly recorded. It would be advisable, although it is not a statutory requirement, for any decision-maker to also consider the NHS Handbook, which gives important background and detail to the information and guidance set out in the Constitution.

11.20. CCGs are subject to an additional duty under section 14P of the NHS Act which states each CCG "must, in the exercise of its functions with a view to securing that health services are provided in a way which promotes the NHS Constitution." The statutory obligation is not to ensure that health services (or education and training) are provided in a way that complies with the NHS Constitution, nor even that they are provided in a way that promotes the NHS Constitution. The duty is to "act with a view to securing" the latter, so it is one further step removed.

11.21. This does not mean, however, that the promotion duties have been entirely insignificant in litigation against NHS bodies. If one can identify a trend from the very few reported cases in which they are cited, it is that the duties to promote the NHS Constitution are being relied on as a sort of reinforcing factor by claimants in the context of claims based on breaches of more specific public law duties.

Sharing data with third parties

11.22. NHS England states that: "the law allows personal data to be shared between those offering care directly to patients, but it protects patients' confidentiality when data about them are used for other purposes. These "secondary uses" of data are essential if we are to run a safe, efficient, and equitable health service. They include:

- Reviewing and improving the quality of care provided;
- Researching what treatments work best;
- Commissioning clinical services; and
- Planning public health services." [107]

11.23. We have already discussed above the legal duties concerning sharing personal data with third parties and the parallel challenges of the general duty of confidence. In respect of sharing information, the NHS recognises that "the duty to share information can be as important as the duty to protect patient confidentiality"[108]. The HSCIC Code of practice on confidential information[109] confirms that:

- All arrangements for sharing of confidential information must be lawful;
- All organisations should be able to demonstrate that their arrangements for sharing of confidential information are lawful;

---

[107] https://www.england.nhs.uk/ig/about/

[108] Caldicott principle 7

[109] https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care/code-of-practice-on-confidential-information

- All organisations sharing confidential information should hold, maintain and publish a data release register;
- The legal arrangements for sharing confidential information should be included in that data release register;
- All arrangements for sharing of confidential information should have regard to:
  - an assessment of the impact of the sharing of confidential information on privacy;
  - the Anonymisation Standard for Publishing Health and Social Care Data[110];
  - the Data Sharing Code of Practice[111];
  - Anonymisation: Managing Data Protection Risk Code of Practice published by the Information Commissioner's Office[112].

11.24. Organisations should only make confidential information available under terms defined in a data sharing contract or agreement for specific purpose(s). Such a contract or agreement will not in itself provide a legal basis but should specify the legal basis. A contract is required where the recipient is not a public body. An agreement will be necessary when sharing with private sector bodies, will apply between NHS bodies and may be applicable between public bodies.

11.25. The Code discusses how information should be shared so that the maximum value can be gained from it, but this concentrates on the operational value – ensuring the proprietary format and structure of the data enable the user to maximise its value, rather than harnessing the value of the data to achieve a financial or commercial return or compensating the original source for exchanging that value. However, the practical guidance setting out how this is to be determined is notably absent.

11.26. Prior to entering into a data sharing contract or agreement for specific purposes the organisation seeking to disseminate confidential information:

- should assess the availability and quality of information and whether that information will meet the intended purpose stated by the proposed recipient;
- should review and understand what steps have been established by the proposed recipient to avoid data linkage, unless the data linkage is necessary to achieve the intended purpose and one or more of the following applies:
  - the person that the information is about has consented; or
  - there is a statutory basis for data linkage, or
  - there is a public interest justification for data linkage, or
  - there is another basis in law for data linkage.

---

[110] https://digital.nhs.uk/data-and-information/information-standards/information-standards-and-data-collections-including-extractions/publications-and-notifications/standards-and-collections/isb1523-anonymisation-standard-for-publishing-health-and-social-care-data

[111] https://ico.org.uk/media/2615361/data-sharing-code-for-public-consultation.pdf

[112] https://ico.org.uk/media/1061/anonymisation-code.pdf

11.27. A data sharing contract or agreement should include:

- the legal basis for disclosure and use
- permitted purposes and manners in which the data will be processed
- whether onward sharing is permitted and on what terms
- arrangements for data destruction once the specified purpose(s) are achieved
- provision for audit of adherence to the contract and/or agreement
- arrangements for data destruction if the terms of the contract or agreement are broken
- penalties if the terms of the contract or agreement are broken
- research publication licence rights, and
- permitted arrangements for linkage to other sources of data.

11.28. Anyone seeking access to Hospital Episode Statistics (HES) data has to submit an application to NHS Digital's Data Access Request Service (DARS), which requires data users to sign up to a data-sharing agreement and adhere to strict information governance protocols (NHS Digital). The Care Act 2014 (2014) added legal restrictions requiring NHS Digital (then the Health and Social Care Information Centre) to disseminate information only if it supports the provision of health and social care or the promotion of health[113].

Examples of failed attempts

11.29. Instances where there have been strong reactions to the NHS' and its partners' approach to sharing data include:

- In 2018, Public Health England (**PHE**) came under fire after handing over records on every case of lung cancer diagnosed in England between 2009 and 2013 (nearly 180,000 lung cancer patients) to William E Wecker Associates, a firm affiliated with tobacco companies. Although the patient data was anonymised, PHE has received backlash for handing over the data without the consent of patients.
- In 2015, researchers at Imperial College London and Ecole Polytechnique CNRS, France, revealed a number of serious flaws with health apps being promoted by the NHS, which had launched a pilot Health Apps Library in 2013. The research study, conducted in 2014, concluded there were "systematic gaps in compliance with data protection principles in accredited health apps". Such failures included: a large proportion of apps did not have adequate privacy policies, a fifth of apps shared limited information, including in some cases details of medical topics that users had viewed or search for, with advertising and marketing companies, some apps sent personal information without the use of encryption and a small number of apps transmitted both unsecured personal and health information, for example research data pairing device and personal identifiers with details of substance use.
- In 2015, the ICO found that Pharmacy2U (the UK's largest NHS-approved online pharmacy) had unlawfully and unfairly sold patients' personal data either directly, or through intermediaries, to scammers. The names and addresses of over 21,500 NHS

[113] Section 261 of H&SC Act 2012

patients, customers of the UK's largest online pharmacy – part-owned by EMIS, the UK's largest GP IT supplier – had been sold to marketers and the ICO issued a Monetary Penalty Notice of £130,000 (notably this fine was issued pre-GDPR).

- In 2017, the Royal Free NHS Foundation Trust provided details on about 1.6 million patients to Google's DeepMind division to develop and refine an alert, diagnosis and detection system that can spot when patients are at risk of developing acute kidney injury. An ICO investigation found several shortcomings in how the data was handled, including that patients were not adequately informed that their data would be used as part of the test. The trust was not fined as a result of the investigation, instead it has signed an undertaking to make changes to the way it handles data.
- In 2013, the HSCIC's (NHS England) care.data programme aimed to extract data from GP surgeries into a central database which would then be used in anonymised form by health care researchers, managers and planners including those outside the NHS such as academic institutions or commercial organisations. Care.data ran into massive problems over the inadequate safeguards it was proposing for the healthcare information it would store on every NHS patient. It was halted by ministers in February 2014, less than a fortnight before the first patient records were due to be extracted, after concerns were raised that patients had not been sufficiently informed about the scheme. The Caldicott review was put in place as a result.

New technologies and dealing with data on commercial terms

11.30. The Kings Fund[114] has identified that whilst digital technology has received significant policy attention in recent years, the provision of funding and incentives for local NHS organisations to pursue digitisation on their own terms has resulted in a locally led approach, which does not necessarily adhere to recognised standards: local NHS organisations could invest in their own technology without it being interoperable with other organisations' systems.

11.31. Fears such as being locked in to a single product or supplier for a range of solutions, along with 'supplier capture' (where suppliers hold long and large contracts which the NHS finds it difficult to get out of) resulted in the DHSC designing a strategy[115] outlining what is needed to enable the health and care system to make the best use of technology to support preventative, predictive and personalised care.

11.32. The strategy seeks to put in place a framework that "allows researchers, innovators and technology companies to thrive, quickly access support and guidance, and develop products that meet user needs" and "create a competitive marketplace for innovation where any tech company can compete and have an equal opportunity to deliver".

11.33. In September 2018, the Initial Code of Conduct for Data-Driven Health and Care Technology[116] was published, with the aim of creating a safe and trusted environment that

[114] 'Clicks and mortar – Technology and the NHS estate' Lillie Wenzel, Harry Evans (2019), https://www.kingsfund.org.uk/publications/technology-NHS-estate

[115] https://www.gov.uk/government/publications/the-future-of-healthcare-our-vision-for-digital-data-and-technology-in-health-and-care

[116] Initial Code of Conduct for Data-Driven Health and Care Technology https://www.gov.uk/government/publications/code-of-conduct-for-data-driven-health-and-care-

encourages innovation and ensures that any benefits from partnerships between technology companies and health and care providers are shared fairly.

"The foundation of any commercial structure should be to ensure that the terms of the engagement fairly allocate the benefits between the parties based on their respective contributions, roles, responsibilities, risks and costs."[117]

11.34. In respect of exclusivity, it states that "**careful consideration should be given before granting exclusivity of access to data**, as exclusivity can limit benefit to the health and care system."

11.35. In terms of value, it states that "Financial value can be realised for the NHS through numerous models, such as simple royalties, free or reduced payments for products, equity shares in the business and improved data sets that can be offered (at a price) to others. However, that is only a part of the value equation. Technology providers derive significant value from the NHS beyond access to unique data sets – through medical and clinical involvement, test beds and pilots – and **this value should be captured within the commercial arrangement**. Further, technology providers may be in a position to generate significant value from any products (or even just from the learning) outside the scope of the initial project, and this value opportunity must be recognised too. Above all the value to patients, clinicians and the wider health and care system should be clearly articulated."

11.36. The Initial Code of Conduct for Data-Driven Health and Care Technology goes on to say that in respect of intellectual property, "where the same algorithm is used in multiple applications; the participant (as data source) in a particular application cannot hope to own the underlying algorithm **but might expect to share in the increase in value**."[118]

11.37. In July 2019, the DHSC published Guidance 'Creating the right framework to realise the benefits of health data'[119] to ensure that the NHS, patients and the public gain fair benefit from agreements involving the sharing of health and care data. It confirms the following guiding principles:

- 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**. Where possible, the terms

technology/initial-code-of-conduct-for-data-driven-health-and-care-technology#principle-10-define-the-commercial-strategy

[117] Initial Code of Conduct for Data-Driven Health and Care Technology https://www.gov.uk/government/publications/code-of-conduct-for-data-driven-health-and-care-technology/initial-code-of-conduct-for-data-driven-health-and-care-technology#principle-10-define-the-commercial-strategy

[118] https://www.gov.uk/government/publications/code-of-conduct-for-data-driven-health-and-care-technology/initial-code-of-conduct-for-data-driven-health-and-care-technology

[119] https://www.gov.uk/government/publications/creating-the-right-framework-to-realise-the-benefits-of-health-data/creating-the-right-framework-to-realise-the-benefits-for-patients-and-the-nhs-where-data-underpins-innovation

of any arrangements should include quantifiable and **explicit benefits for patients** which will be realised as part of the arrangement;

- 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**;
- 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;
- 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;
- 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.

11.38. The Guidance goes on to emphasise that NHS organisations should not enter into agreements which grant one organisation sole (exclusive) right of access to or use of raw NHS data, either patient or operational data. The above principles are intended to cover agreements involving data entered into by all NHS organisations, at the primary (GPs), secondary and tertiary care levels, including relevant data from organisations contracted and funded to deliver NHS services. It is not clear to what extent the guidance applies to organisations working alongside the NHS to deliver health and social care services. The principles are designed to apply to agreements which include a commercial partner or where the outputs could be commercialised, regardless of the type of organisation the NHS is partnering with.

11.39. In December 2018, NHS Digital published a draft new NHS Digital, Data and Technology Standards Framework[120], which describes its new expectations around the use of data, interoperability, and design standards within the NHS[121]. It confirms that NHS digital, data and technology services should be contracted for in accordance with the NHS Digital's Commercial and Behavioural Principles[122] such as: mitigating against any real or perceived conflict of interest through suppliers' work with the NHS.

11.40. The principles highlight that "a supplier with a position of influence gained through their relationship with any part of the NHS should not use that position to unfairly

[120] https://digital.nhs.uk/about-nhs-digital/our-work/nhs-digital-data-and-technology-standards/framework

[121] https://digital.nhs.uk/about-nhs-digital/our-work/nhs-digital-data-and-technology-standards/framework

[122] https://digital.nhs.uk/about-nhs-digital/our-work/nhs-digital-data-and-technology-standards/framework/beta---commercial-and-behavioural-principles

disadvantage any other supplier or reduce the potential for future competition, for example by creating a technical solution that locks in the supplier's own goods or services." Regarding pricing, "contracts should be priced to offer sustainable value throughout their life, including when changes are needed. Whilst [it is accepted that] suppliers need to make a profit margin in return for the risk they are accepting, [NHS Digital] expect suppliers not to exploit an incumbent or monopoly position, an urgent situation or an asymmetry of capability or information to impose opportunistic pricing."

Suppliers are expected to mitigate against any real or perceived conflict of interest through their work with the NHS and must not use their position to unfairly disadvantage any other supplier or reduce the potential for future competition.

11.1. In addition to NHS-specific guidance, the Social Value Act 2012[123] requires public sector commissioners – including local authorities and health sector bodies – to consider economic, social and environmental wellbeing in procurement of services or contracts.

11.2. This is particularly important when considering the elevated status of trust the NHS holds in the eyes of the public. "While there is a core group of people who do not want this health data shared at all, many people find that sharing health data with commercial organisations is acceptable if there is a clear public benefit for this sharing. A clear public benefit is often seen to be, for example, something with a clearly medical aim, such as developing treatments and, in some cases, improving health services."[124] In contrast, the public consider that where no benefit to public health is perceived, commercial access is unacceptable[125].

11.3. It is important to recognise that "the social benefit of commercial access is not always apparent at the start of the deliberation process, so people either focus on risks to themselves or exaggerate the public risk and fear the worst of private sector involvement. Without a clear conception of how the public stand to gain, the public cannot carry out their internal trade-off exercise and weigh up public good against personal risk. They often revert to their pre-existing stereotypes about government and business in the absence of more knowledge."[126]

---

[123] An introductory guide to the Public Services (Social Value At) 2012 for commissioners and policymakers can be found at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/690780/Commissioner_Guidance_V3.8.pdf

[124] https://www.ipsos.com/ipsos-mori/en-uk/commercial-access-health-data

[125] The One-Way Mirror: Public attitudes to commercial access to health data', Ipsos Mori report prepared for the Wellcome Trust (2016) https://www.ipsos.com/sites/default/files/publication/5200-03/sri-wellcome-trust-commercial-access-to-health-data.pdf

[126] 'Accountability, transparency and public participation must be established for third-party use of NHS data' https://understandingpatientdata.org.uk/news/accountability-transparency-and-public-participation-must-be-established-third-party-use-nhs

Conclusions:

- Sharing data with third parties, including for-profit organisations is not prohibited, provided the NHS can realise the value of that asset transfer – whether that involves a financial payment or some other opportunity to realise a social benefit for the public.
- Current guidance and frameworks emphasise the need to recognise the value of data shared with third parties but offer no assistance with determining the value of the data.
- It is unlikely that individuals can bring legal action for their data being sold at an 'undervalue' but they can bring action for breaches of their rights such as the loss of control over their data.

APPENDIX

REFERENCES

KEY LEGISLATION

- **Care Act** 2014
- **CDPA** Copyright, Designs and Patents Act 1988
- **the Convention** the European Convention for the protection of Human Rights
- **DPA** Data Protection Act 2018
- **Equality Act** 2010
- **GDPR** General Data Protection Regulations 2016
- **H&SC Act** Health and Social Care Act 2012
- **Health Act** 2009
- **HRA 1998** Human Rights Act 1998
- **MCA** Mental Capacity Act 2005
- **NHS Act** 2006
- **PA** Patents Act 1977
- The Public Contracts Regulations 2015
- The Re-use of Public Sector Information Regulations 2015
- The Social Value Act 2012
- Trade Secrets (Enforcement etc) Regulations 2018

GLOSSARY

- **CAG** Confidentiality Advisory Group
- **HDRUK** Health Data Research UK
- **HRA** Health Research Authority
- **ICO** Information Commissioners Office
- **IP Address** Internet Protocol address
- **IPR** Intellectual Property Rights
- **MRC** Medical Research Council
- **TTP** Trusted third party

If you have any queries or comments in regard to this document please contact:

Emma Watt
Associate
Tel: 0121 214 3609
Email: emma.watt@anthonycollins.com

Anthony Collins
solicitors

Anthony Collins Solicitors LLP
134 Edmund Street | Birmingham | B3 2ES
www.anthonycollins.com | https://newsroom.anthonycollins.com