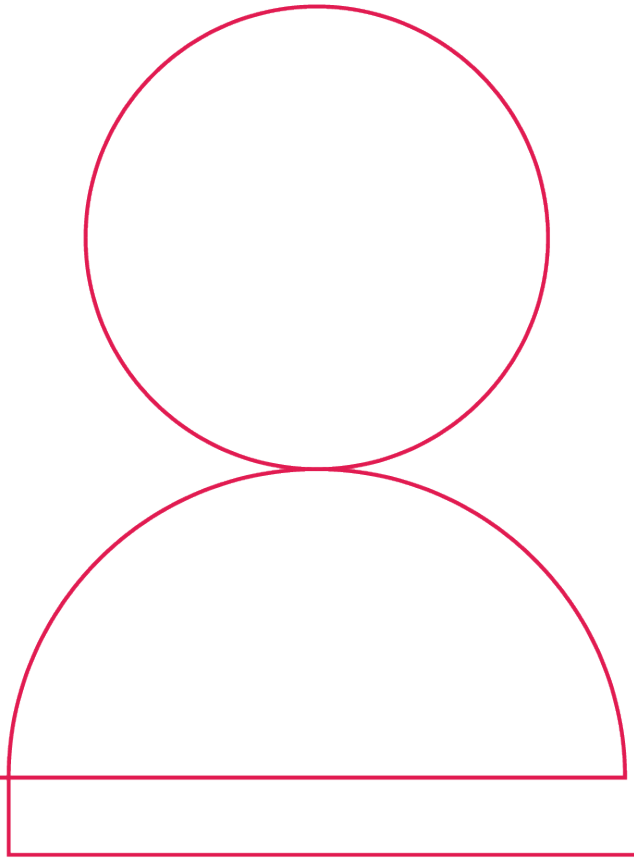
Academy of Medical Royal Colleges

June 2021

Disclosing personal demographic data: The public interest

Report of a seminar held at the Academy of Medical Royal Colleges



Contents

Executive Summary

In January 2020, the Academy of Medical Royal Colleges convened a workshop to discuss public interest disclosures to government agencies of Personal Demographic Data (PDD) held by the NHS. PDD is distinct from clinical information: it contains only demographic details, such as name and address, and does not disclose information about health. Protecting patient information is of the utmost importance, and disclosures of confidential data are regulated by a robust legal framework. Within this framework, disclosures can be made if judged in the public interest.

Making this judgment involves using a 'public interest test' — a process of identifying and weighing potential benefits and harms of disclosure. But there is relatively little guidance on what factors are relevant and how they might be judged in light of one another. We invited representatives from several domains, including the health service, patient groups, government, data protection and human rights, to help elaborate the framework for this important test.

A preliminary question is whether PDD is confidential and therefore even requires a public interest test. We recommend PDD in the health system continue to be considered confidential for the present. Confidentiality, however, can be affected by the context in which information is provided and the expectations of the patient. Further work to understand different contexts and expectations could help progress the question.

When making public interest decisions for NHS PDD, we found the following factors are potentially relevant to disclosure: to prevent physical or mental harm to individuals, including cases where the data subject is vulnerable; to prevent harms caused by criminal behaviour, such as fraud and immigration offences; to improve the functionality of public services, for example less intrusive management of the tax system or more efficient regularising of immigration status. These do not provide justifications in themselves but are reasons that could be included in a public interest test.

The main factors that weigh against disclosure are: the potential for trust in the NHS to be undermined; the risk that people will not seek care if they worry their data will be shared; the risk to public health if individuals do not seek care; compromising the ethical standing of medical professionals; and the risk that the health system becomes incorporated more routinely into the other functions of the state.

There is little to no guidance on what gives factors greater or lesser weight when it comes to judging them in light of one another. While balancing factors for disclosure against those for non-disclosure is always specific to the circumstances of each case, we suggest the following criteria might give more weight to the factors for disclosure (the factors for non-disclosure are relatively static).

Factors have more weight if:

- Injury is imminent and certain.
- Injury is particularly large e.g. large-scale fraud.
- Nature and intention of the perpetrator is especially malign e.g. organised crime.
- Financial injury is against the NHS.
- Disclosure more conclusively meets the proportionality test.
- Disclosure obviously supports what the individual thinks is in their interest.

Factors have less weight if:

- Injury is identifiable only in very general, uncertain or indirect terms.
- Data usage less conclusively meets the proportionality test.

Formalising and improving the transparency of procedures through which public interest assessments are made would help to reassure citizens their information is used responsibly by public bodies.

Introduction

The law allows for confidential information to be shared when there is a public interest in its disclosure that outweighs any interests in keeping the information confidential. But it does not provide definitive or exhaustive guidance on what constitutes a sufficient public interest to justify disclosures. The Academy of Medical Royal Colleges convened a workshop to discuss this in relation to disclosures to government agencies of personal demographic data (PDD) held by the NHS. The purpose of this report is to provide a factual, neutral representation of the opinions expressed.

The aim is to have an analysis of the central issues that pose a challenge to this complex subject, as well as a record of the different positions that exist. As information sharing continues to increase, it is more important than ever to consider the circumstances in which data disclosures could be made. If not, disclosures run the risk of reflecting arbitrary decision making or the use of information according to narrow interests.

Drawing together the commonalities and differences of opinion, therefore, is an attempt to move towards a more objective framework in which the competing interests present in a potential data disclosure can be recognised and balanced against one another and the processes for making such assessments can be regularised as far as is possible. It is hoped that the factors raised and discussed in this report may act as a reference point for those making public interest assessments in the future.

The report is structured in two parts. The first section asks whether PDD is confidential. This question is important, because where information is confidential it might only be permissible to disclose on the basis of a thorough assessment of the relevant public interests. The second section discusses the requirements for a PDD disclosure to be deemed in the public interest.

Assessing the public interest is a particularly difficult task. First, the different interests present in a potential disclosure — on the part of the individual whose data is being disclosed as well as the interests of other individuals and society — must be identified. Following current public interest test frameworks, these interests have been roughly categorised in the report into benefits and harms.[1] To draw out some of the factors that might be relevant when considering the benefits of disclosure, at the workshop the National Crime Agency, NHS Counter Fraud Authority and HMRC presented case studies of potential uses of PDD. The author interviewed the Home Office for the fourth case study. The potential harms of disclosing PDD were well articulated by other attendees.

Once interests have been identified, they must then be weighed against one another to determine where the balance of interest lies. This is potentially a highly subjective task, but it does take place in the light of certain general principles, provided by the law or by widely accepted norms, that suggest which arguments carry more weight in the balancing test. In this report, therefore, the discussion of

1. 'Disclosing information in the public interest' [Para 63-70] of the General Medical Council's Confidentiality: good practice in handling patient information https://www.gmc-uk.org/ethical-guidance/ethical-guidance-for-doctors/confidentiality/disclosures-for-the-protection-of-patients-and-others#paragraph-60 [Accessed 1 Jan 2020].

harms and benefits is bookended first by a general framing of the public interest and last by an assessment of some aspects which may give factors more weight. These aspects were not articulated in explicit terms by workshop attendees but have been reached by interpreting why one argument appeared more persuasive to attendees than another.

The report includes perspectives that were commonly held by workshop participants and those that were voiced by only one person. The reason for including the views of an individual person is usually because the single perspective provided a novel viewpoint which may be of interest in future discussions. It has been made clear where the position was expressed by just one individual, so that these are not thought to necessarily represent a wider base of opinion.

Finally, the theme of trust was an important one for all attendees: trust in the NHS, in the professionals that work in the NHS, and in the government agencies that are ultimately democratically accountable to the public. Trust was recognised not just as an important value in its own right but also functionally necessary for the healthcare system, since confidence in its services supports treatment and protection of individual and public health. Individuals or organisations assessing whether to use confidential information in the public interest are therefore responsible for acting in a manner which supports relationships of trust. This does not mean decisions cannot be taken in the public interest that members of the public may not like or agree with, but that the integrity and justifiability of the decision and decision-making processes must be respected by those making them.

Confidentiality of Personal Demographic Data

Confidentiality of information in the NHS is governed by a complex framework that includes legal principles and provisions, professional codes of practice and regulatory guidance. Underpinning these is the well-established principle that the duty of confidentiality arises from the receipt of information that is expected to be treated as confidential. The law strongly protects such information, permitting its disclosure only for certain reasons.

Generally, confidential information may be disclosed: if consent has been given, which includes explicit consent as well as implied consent for direct care in the health and care context; if the data controller[2] is obligated by a court order or legislation such as the Serious Crime Act 2007; or if permissive legislation provides a gateway for a public body to disclose information. Finally, if none of these reasons apply, a disclosure of confidential information may still be acceptable if it is judged to be justifiable in the public interest.

The information held by the NHS includes clinical information and Personal Demographic Data (PDD). PDD is demographic information, such as name, address, date of birth and NHS number, and does not disclose information about health. The confidentiality of clinical information is unquestioned, but doubts have been raised about PDD. This matters, because if PDD is not considered confidential information, there would be no legal requirement to undertake a public interest assessment before disclosure to meet the duty of confidentiality. Public interest assessments become relevant if PDD is considered confidential and where there is no other legal justification or requirement to disclose.

The following discussion uses an analytical distinction made by attendees between confidentiality based on the *content* of information or the *context* in which it is given. The perspective of the patient seeking care is also crucial to both, reflecting the patient-centred — rather than paternalistic — orientation of healthcare in recent years. The final part of this section, therefore, comments on the 'reasonable expectations' of privacy on the part of the patients who have disclosed the PDD, a concept developed in case law.

2. The 'data controller' is defined in the General Data Protection Regulation as the natural or legal entity which determines the purposes and means of the processing of personal data. Guide to the General Data Protection Regulation (GDPR) [Accessed 3 March 2021] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

Confidentiality based on Information Content

Judged on its content, most attendees thought that PDD gathered through healthcare practice must be considered confidential in all circumstances.

The opinion was that legislation, professional guidance and case law examples do not recognise a distinction between PDD and clinical information.[3] The *National Health Service Act 2006* defines patient information as confidential in circumstances when:

> *the identity of the individual in question is ascertainable (i) from that information, or (ii) from that information and other information which is in the possession of, or is likely to come into the possession of, the person processing that information, and (b) that information was obtained or generated by a person who, in the circumstances, owed an obligation of confidence to that individual.*[4]

Most attendees thought that when creating the legislation Parliament did not intend to differentiate between health-related information and PDD. Other guidance, such as that published by the General Medical Council and the British Medical Association, does not recognise a difference between the two.[5] Several also referred to the Court of Appeal's judgement in W, X, Y and Z, which referred to the definitions of confidential information in the General Medical Council's Standards and Ethics Guidance, the NHS Code on Confidentiality and the British Medical Association's 'Confidentiality and Disclosure of Health Information tool kit' to conclude that:

> *In our view, all of these documents articulate the same approach to the issue of confidentiality: all identifiable patient data held by a doctor or a hospital must be treated as confidential.*[6]

The confidentiality of PDD based on content can be considered in light of patient expectations. Some attendees stated that members of the public would likely assume no differentiation is made between clinical information and PDD and queried how such a distinction could be explained to patients. A corollary concern was that were such explanations to become necessary, the responsibility would be placed on GPs, whose consultation time with patients is limited. Putting doctors in the position of advising patients that some of their information would not be confidential also risks disrupting the relationship of trust that all agreed was important.

A counterview was that PDD cannot be considered sensitive information. One attendee noted that most people give out personal demographic information willingly to many different organisations or services, including government agencies, retail outlets, and online services. Patients might not therefore reasonably expect such data to be kept confidential by the NHS.

Confidentiality based on Information Context

For many attendees, considering the context in which information is provided is a more profitable way of thinking about confidentiality, since what the data is does not really make explicit when a duty of confidentiality is owed. In the words of one attendee, 'information that is disclosed or collected by health and social care services may be information that is known by many others or is freely available from other sources. The relation of confidence, however, ought not to take that into account.' This opinion directly disputes the counterview above.

3. Some suggest that this distinction is made in the NHS Act 2006. In s.251(10), 'patient information' is defined as: '(a) information (however recorded) which relates to the physical or mental health or condition of an individual, to the diagnosis of his condition or to his care or treatment, and (b) information (however recorded) which is to any extent derived, directly or indirectly, from such information, whether or not the identity of the individual in question is ascertainable from the information.' However, not all accept that purely demographic information would fall outside of the scope of this, nor that the definition of 'patient information' in s.251 should anyway determine all the types of information that are owed a duty of confidentiality.

4. National Health Service Act 2006 s.251(11)(b) [Accessed 16 February 2020] http://www.legislation.gov.uk/ukpga/2006/41/section/251.

5. 'Confidentiality'. British Medical Association. [Accessed 12 March 2020] https://www.bma.org.uk/advice/employment/ethics/medical-students-ethics-toolkit/9-confidentiality; 'Confidentiality: good practice in handling patient information'. General Medical Council. [Accessed 12 March 2020] https://www.gmc-uk.org/ethical-guidance/ethical-guidance-for-doctors/confidentiality.

6. W, X, Y and Z v The Secretary of State for Health. [2015] EWCA CIV 1034 [39]. https://www.judiciary.uk/wp-content/uploads/2015/10/w-x-y-z.pdf.

One of the primary factors for assessing context is the reasonable expectations of the individual. The question is whether in the health and care system patients should have reasonable expectations of confidentiality with regard to their PDD in all contexts in which it is disclosed and if there are circumstances in which they would not or could not have such expectations.

For some attendees, thinking about confidentiality through the context lens did not change the fact that PDD should be considered confidential in all circumstances. The doctor-patient relationship is well established as one in which a duty of confidentiality is owed and therefore one in which patients expect their information to be treated as confidential. Another view focused on the purposes for which the information was given: as the data is collected for the provision of health and social care, the individual seeking care would not expect their information to be used for another purpose.

However, understanding confidentiality as contextually based does create at least the prospect of circumstances in which the duty of confidentiality does not apply. One attendee suggested that the obligation of confidentiality was not in theory absolute and might be defeated if a patient entered the relationship of confidentiality deceptively, such as by deliberately giving fraudulent details about an illness or falsely claiming medication for a deceased relative. Others accepted more generally there might be circumstances in which grounds did not exist for reasonable expectations of privacy.

Reasonable Expectations

Crucial to both ways of thinking about confidentiality is a consideration of the reasonable expectations of the patient. The content-based understanding of confidentiality requires knowledge of whether a patient expects their PDD to be as confidential as their clinical information. The context-based perspective puts the concept of reasonable expectations as one of the central factors determining if a context creates a duty of confidentiality. The two are interrelated: it could be the case that a patient has no actual expectation of their PDD being confidential in the context of providing their information to a hospital because they view name and address information as something they widely share.

Ascertaining the reasonable expectations of patients is not simple. It cannot be assumed that notifying individuals that information might be disclosed is sufficient to qualify the disclosure of information as 'reasonably expected'. Additionally, what patients ought to reasonably expect is not synonymous with what patients do expect, although the two should not be entirely distinct.

Some attendees were uncertain that public and patient views are sufficiently understood. NHS Digital conducted a survey in 2018 measuring people's expectations of the confidentiality of their medical records and found 97% of people thought the NHS should treat address information confidentially.[7] Attendees agreed, however, that people's expectations change over time. In the past few years, awareness of information sharing has grown significantly, and public attitudes may also have shifted. Some attendees suggested the perception of what the public reasonably expects in relation to the NHS is driven by the response to high profile media issues in specific cases and that the intervention of advocacy groups opposed to the use of data is not reflective of the general mood.

The belief that people have become more knowledgeable about information sharing should not be overstated. Research into public attitudes about data commonly finds low awareness of how patient data is used beyond individual care.[8] One attendee thought patient groups, which represent the interests of patients with a specific disease or condition, may have a range of views about what might legitimately be shared, but neither their knowledge nor opinions are necessarily representative of the public at large. In addition, the quality of information provided to the public is highly variable, despite valuable work done by several organisations, such as Understanding Patient Data. Uncertainty is therefore present on both sides: in the system's understanding of what patients reasonably expect and in patients' understanding of what happens with their clinical and demographic information.

The general importance of patient expectations has been underlined by the National Data Guardian, who recently added a Caldicott Principle which makes clear that patient and service user expectations must be considered and informed when confidential information is used.[9]

7. 'NHS Digital statement on Health Select Committee's report into patient data sharing'. NHS Digital. [Accessed 12 March 2020]. https://digital.nhs.uk/news-and-events/latest-news/nhs-digital-statement-on-health-select-committees-report-into-patient-data-sharing.

8. 'Public attitudes to patient data use'. Understanding Patient Data. [Accessed 12 March 2020] https://understandingpatientdata.org.uk/sites/default/files/2018-08/Public%20attitudes%20key%20themes_0.pdf.

9. 'The Caldicott Principles'. The Caldicott Principles - GOV.UK (www.gov.uk)

Conclusion

Whether and when PDD should be considered confidential continues to attract different views. Although classifying information based on content appears to provide a neat answer to this problem, most attendees felt it unsatisfactory, because the duty of confidentiality arises in the context of the relationship in which information is provided. This circumstantial character entails that information which might not be confidential in one context becomes confidential in another. Conversely, it allows that information given by the patient to the health and care system might not be confidential in all contexts.

The most dominant view was that there should be a default presumption of confidentiality. Half of attendees on the day concluded that PDD should always be considered confidential, while a third thought that it was confidential in certain circumstances. These figures are not conclusive evidence of the weight of opinion on this matter and do not capture the complexity and nuances of the subject. They do, however, provide an indication that it is highly unlikely PDD can be thought of in blanket terms as not confidential.

Overall, there may be a need to nuance the discussion of confidentiality. One aspect of this would be to identify the factors that determine the contexts in which PDD is confidential, for example when the patient would have a reasonable expectation of privacy. Attendees agreed that further research to understand public expectations could be helpful, particularly if it contributed to a broader project of public education about the use and disclosure of NHS data. It might therefore be useful to conduct a large-scale survey to measure public perceptions which sets out some proposed uses of data to compare public sentiment in each case.

Finally, to return to the question of explaining distinctions, if PDD were considered non-confidential in some circumstances, there might be a need for more collective responsibility in undertaking these kinds of discussions with the public and patients. Attendees suggested that it should not fall exclusively to the NHS and its professionals to explain such distinctions.

Public Interest Assessments

Workshop attendees did not reach complete consensus on the confidentiality of PDD. However, all agreed that the duty of confidentiality could legitimately be breached in certain circumstances and for certain well-defined purposes, one of these being the existence of a strong and convincing public interest in so doing which outweighs the interests in maintaining confidentiality. The main focus of this report is the public interest justification for NHS organisations disclosing confidential information to government agencies.

Undertaking a public interest test requires balancing multiple, competing interests. Interests can be categorised roughly in terms of the benefits to individuals or society in disclosing confidential data in a particular circumstance and the harms to the individual whose data is disclosed, as well as the broader harms to society in breaching confidentiality. Attendees warned against being misled by this balancing act into a mere utility calculation, stating that the importance or weight of interests, such as the maintenance of trust between a health professional and a patient, must be appreciated as having wider ethical significance. This does not, however, invalidate the act of seeking to understand the competing interests that are at stake and weigh up their relative importance in a particular instance. If done properly, this process in fact helps to support those undertaking public interest tests recognise that in any assessment there will be multiple interests to consider.

The challenge for those undertaking such assessments is that although there are pieces of guidance that provide some advice on the kinds of factors that should be considered, there is no comprehensive list of factors that can be applied to situations, nor a definitive framework to determine the balancing exercise. The workshop in 2020 aimed to initiate a discussion on this gap and, through this report, to act as a starting point or reference for those making assessments in the future.

The following section covers: first, the concept of the 'public interest', which frames how different interests are interpreted; second, case studies of PDD usages; third, the benefits and harms of such disclosures; fourth, the factors that give more or less weight to benefits and harms in the balancing test; and fifth, reflections on public interest test procedures.

The Public Interest

A useful starting point for considering what is meant by the term 'public interest' is the Information Commissioner Office's (ICO) guidance on public interest exemptions from information disclosure in response to Freedom of Information requests.[10] The ICO's guidance is directed towards a different end, but its general principles are applicable, and many were implicitly referred to by workshop attendees.

10. 'The Public Interest Test'. Information Commissioner's Office. [Accessed 12 March 2020]. https://ico.org.uk/media/for-organisations/documents/1183/the_public_interest_test.pdf

The first relevant general principle referred to by the ICO is that the public interest refers to the public good, not what is of interest to the public. The public good is a difficult, abstract term to define, but attendees recognised that the public good should consider what the public thinks is in the public interest. It might therefore be informed by democratic political mandates, such as an elected government's promise to focus on policing, immigration or some other element of law enforcement. However, most felt this is in itself an insufficient way of determining the public good. First, the majority view is not the only one that should be taken into consideration. The rights and the protections afforded to minorities are also an equally valid and important part of what constitutes the public good. Second, policy decisions are not infrequently made which might diverge from majority opinion but are deemed to be necessary for the public's protection or wellbeing.

The public interest test operates within a context of legal, ethical and social norms, which must be taken in the round to do justice to the concept of the public good. Attendees noted such norms would involve institutional integrity, for example complying with law, ensuring that publicly funded bodies carry out their functions fairly and impartially, acting 'reasonably' in accordance with public duties and associated purposes of governance, and ensuring accountability and transparency in relation to the public purse. Attention was drawn to the ethical claims attached to maintaining confidentiality, which involve the autonomy of the individual (the respect for patient values, wishes and choices), the promises made to people by the system which set up expectations of confidentiality, and the standards of confidentiality which underpin patients continuing to seek care from the health service. On the other side, the ethics of disclosure entail that individuals recognise there are limits to their autonomy when there is good reason and may accept disclosure if careful consideration has been taken of the full range of foreseeable harms and the range of people who might suffer those harms.

Disclosures must also meet legal principles developed by the European Court of Human Rights. This requires that the infringement of privacy must have a legitimate aim, such as national security, prevention of disorder or the interest of the domestic economy, and that there is a pressing social need. Further to this, the UK Supreme Court has developed a proportionality test, which asks if the objective is sufficiently important to justify the interference, if the measure is effective in meeting the objective, if a less intrusive measure could reasonably be used, and if a fair balance has been struck between the rights of the individual and the public interests. These legal principles provide an indication of what constitutes the kind of exceptional reason that the ethics of confidentiality demands. Judging benefits and harms should also take into account the likelihood of them occurring.

This complex environment means that the public interest must be assessed on a case-by-case basis, which is a second principle referred to by the ICO. Public interest assessments are inherently a matter of case-by-case judgment, and the balancing of factors favouring disclosure or non-disclosure will always depend on the circumstances of the case. Although it is possible, and perhaps desirable, to stabilise some public interest factors and aspects which affect their weighting, there will always be a need for flexibility and careful consideration of the particular case in question.

Case studies

For the purposes of this report, four government organisations, the National Crime Agency, NHS Counter Fraud Authority, Her Majesty's Revenue and Customs and the Home Office,[11] were invited to contribute information about current or potential use of NHS PDD and provide opinions on why such uses of data were in the public interest. The intention in presenting these case studies was not to conclude whether in these scenarios data could or could not be disclosed in the public interest. It was instead to put forward some factors that could be relevant when making such assessments and to bring into deliberation the key evaluative themes, including severity of harm and the proportionality and effectiveness of data use.

National Crime Agency

The National Crime Agency (NCA) uses NHS data for the purposes of tracing and finding fugitives circulated on European arrest warrants, a situation in which organisations are compelled to provide confidential information to support criminal proceedings. Although this is therefore an example that does not rely on the public interest test to authorise the disclosure of confidential data, it shows how standards and principles of disclosure can be used in straightforward cases. A specific case explained was the use of NHS data to support tracing a foreign national who had targeted elderly

11. The National Crime Agency, NHS Counter Fraud Authority and Her Majesty's Revenue and Customs attended the workshop on 17 January 2020. The Home Office provided its contribution through an interview with the author in February.

people with high-level fraud worth millions of pounds. The individual had been wanted for this offence for ten years when the NCA was made aware he had started a company in the north of England.

The NCA official stated the use of data was proportionate by explaining that decisions about data use focus on achieving the desired outcome with the minimum amount of intrusion. The agency uses information already known to the organisation and publicly available information. Only after this are requests made for information to organisations such as the NHS. The NCA referred to the effectiveness of the data usage by arguing that although fugitives generally remain well hidden, they still often use public services. The official noted that, contrary to popular perception, the agency does not have quick and straightforward access to resources such as telecommunications data. Often the simple checks, such as the use of NHS services, are the most effective.

NHS Counter Fraud Authority

NHS Counter Fraud Authority (NHS CFA) spoke about the potential use of NHS data to address fraud in the NHS. Since NHS CFA has separate legal powers to access NHS data to address individual cases of fraud for specific criminal investigations, this case study referred to using tranches of NHS data for analytics.

NHS CFA stated that fraud is a difficult crime to address since it is by its nature hidden. Tranches of NHS data, however, could be used directly to identify fraud in the NHS or to devise a methodology for identifying fraud, which could then be run through the full dataset by the data controller. This would minimise the data disclosed to the NHS CFA while helping to eradicate fraud from the system.

NHS CFA indicated the severity of the crime by stating it estimates fraud costs the NHS over £1 billion a year and that the NHS is being increasingly targeted by organised crime groups. Officials referred to proportionality by highlighting that the amount of data provided to NHS CFA could be kept to the minimum necessary for developing analytical tools and methodologies. They noted it is not possible to use data other than NHS data, as the purpose is to tackle NHS fraud in the NHS system. A partnership with NHS Business Services Authority had yielded £16.8 million in value to the NHS, indicating the effectiveness of such methods.

Officials thought NHS CFA's claim to the use of PDD was especially significant because the agency's purpose is to safeguard the NHS from fraudulent behaviours that impede the ability of the system to provide care to the public. In their view, NHS fraud is therefore intrinsically linked to the treatment of NHS patients. Reasons to address fraud are not limited to ensuring protection of the public purse but also to prevent public safety issues. The position of NHS CFA is that this is both overwhelmingly in the public interest and additionally consistent with the principles of the NHS itself.

Her Majesty's Revenue & Customs

HMRC provided two examples of potential uses of NHS data, stating that it had not made representations to NHS data controllers for any such information. The two examples given were the use of data to corroborate suspected cases of fraud and the use of large quantities of data to improve tax compliance across the system.

In the first case, officials stated that PDD can be useful for two main purposes: to identify individuals operating in the hidden economy; or to tackle attacks on the tax and benefits system by organised criminal gangs. A group might claim money by asserting a certain number of people live at an address. NHS address information could be used to corroborate whether this is true. For the second case, officials referred to the growing push across government for departments to share information for counter-fraud analytics, as facilitated by the Digital Economy Act.

HMRC holds its own substantial amounts of data on taxpayers and acquires information from several other departments to support its work. Officials advised that the use of NHS data was therefore not a matter of necessity but of increasing effectiveness, as it is the use of multiple different datasets to enable cross-comparison that make it possible to determine if a claim is incorrect or fictitious.

Home Office

The Home Office provided information about using PDD to help trace certain individuals who are required to maintain contact with the Home Office, but who have ceased contact and are in a situation of vulnerability or present a serious harm to the public. Immigration officials work with many organisations, both governmental and non-governmental, to provide support in these cases where

there are safeguarding and welfare concerns.[12] The Home Office advised that it uses information from multiple agencies to trace individuals making use of NHS PDD only when other sources of information have not been sufficient. The use of NHS data is therefore highly specific, involving caseworkers and internal review procedures that assess the use of such information on a case-by-case basis, confirming where individuals have committed serious offences or there are safeguarding concerns.

The Home Office also provided information about tracing more generally individuals who have ceased contact with Immigration Enforcement. All migrants are expected to comply with the Immigration Rules, regularising their stay or leaving the UK when required. The Home Office advised that some migrants are expected, and legally required, to report to the department as part of their conditions of being in the UK. In such cases where people have ceased to maintain contact, it requests information from other government departments, such as HMRC and the Department for Work and Pensions, to retrace those individuals. Department representatives articulated several potential outcomes of this process. The individual might be granted immigration leave in the UK, and officials advised that it can be the case that tracing is required simply to resolve such cases. Another outcome is that the individual might be given support to return to their home country voluntarily, which officials noted is not an unusual occurrence. Finally, individuals may be removed if there is no basis for granting them further leave to remain.

The Home Office stated that this assistance has benefits that should be considered in a public interest test for PDD. The first is that one of the department's most important functions, and a capacity unique to the organisation, is its ability to regularise status. This, officials stated, was of significant interest to the individual, as regularised status is necessary for being able to gain employment and other benefits enjoyed by citizens. This is also particularly important in the case of children for whom a lack of such status would present multiple difficulties on entering adulthood. Lack of legal status can leave individuals open to exploitation in the illegal labour market, for example. Second, individuals seeking to evade immigration enforcement may make use of services and welfare support they are not entitled to. They therefore stated there is significant public interest in enforcing immigration law, including for the purposes of driving down exploitation, protecting the public from harmful individuals and preserving public funds.

Benefits

By considering the benefits of specific data disclosure based on already existing guidance and the case studies set out above, this section suggests some relevant factors for disclosure.

The potential for morally significant benefit to individuals, attendees agreed, is the strongest reason to permit data disclosure i.e. *to prevent serious, imminent physical or mental harm*. This covers disclosure to investigate or prevent a range of violent crimes, including terrorism, murder, manslaughter, rape, treason, kidnapping, and child abuse. Attendees also considered other instances of safeguarding, such as protection from modern slavery, and agreed that the protection of vulnerable individuals would constitute a good reason for breaching confidentiality. Such factors might be relevant in some examples presented by the Home Office, but attendees thought vulnerability may not be a justifiable reason for disclosure to the Home Office specifically, as the disclosure might be better made to another organisation, such as the local authority.

It is widely recognised in professional guidance and codes of practice that confidential data may be shared in the context of a serious crime, but beyond obvious cases evaluating the severity of harm, and therefore its weight in balancing competing interests, becomes more difficult.[13] No definitive list exists of which crimes should be considered serious, nor clear guidance as to what factors set the threshold of severity. Some attendees proposed that terms could be defined more clearly and a comprehensive reference list compiled. This might be difficult, since specific circumstances are often determining factors, but if a definition were to be developed, one question raised was who would set any new criteria—for example, Parliament or senior, highly trained individuals from relevant disciplines [for example psychiatrists, police and counter fraud specialists].

12. This section refers both to practices under the [now withdrawn] Memorandum of Understanding [MoU] between the Home Office, NHS Digital and the Department for Health and Social Care, which came into effect 1 January 2017, and after changes were made in May 2018 to the arrangement. These changes substantially narrowed the number and scope of data sharing requests. Before practice changed, the MoU facilitated tracing requests to NHS Digital to locate immigration offenders. After May 2018, a very small number of tracing requests have been made on a highly specific case-by-case basis where there is a strong interest in doing so because of safeguarding and welfare concerns.

13. The factors 'harm' and 'serious harm' are frequently interwoven or used synonymously with 'serious crime'. This is because, to the extent that a definition exists, serious crimes tend to be explained in terms of their harms to individuals or to society.

Some definitions of serious crime already exist. The *Confidentiality: NHS Code of Practice Supplementary Guidance: Public Interest Disclosures* advises serious crime, *'will include crimes that cause serious physical or psychological harm to individuals. This will certainly include murder, manslaughter, rape, treason, kidnapping, and child abuse or neglect causing significant harm and will likely include other crimes which carry a five-year minimum prison sentence but may also include other acts that have a high impact on the victim.'* [14] The *Confidentiality: NHS Code of Practice* brings other potential harms into scope, advising that, *'serious harm to the security of the state or to public order and crimes that involve substantial financial gain or loss will also generally fall within this category.'* [15] This definition invites consideration of a broader set of potential circumstances under which it might be appropriate to disclose data.

The NHS CFA and HMRC case studies stimulated a discussion among attendees on the justifiability of some of these, especially the case of fraud.[16] In both, some of the benefits to individuals and society in disclosing the data were articulated in terms of the *protection of public services and the public purse from criminal activity*. Citizens, this position states, have an interest in taxpayer-funded services not losing money to criminal activity, particularly organised crime. In the case of HMRC, tax compliant individuals will want to know that tax is properly managed and controlled so that they can benefit from public funds being spent on public services like the NHS. In the NHS CFA case, individuals may have an interest in tackling fraud in the NHS system to support the funding of treatments and healthcare services from which they benefit.

The case studies proposed other benefits. The HMRC suggested that one benefit of its use of PDD would be *reducing the degree of visible intrusion experienced by individuals* as HMRC executes its functions. Routine use of data for promoting tax compliance, for example, might mean a reduction in individuals mistakenly paying an incorrect amount of tax. The ability to corroborate suspected cases of fraud might also minimise the initiation of intrusive and stressful investigations. Alternative benefits to individuals in disclosures of data to support the activities of NHS CFA were expressed in terms of *patient safety*. In one instance of fraud, for example, an individual had resold non-sanitised products to a hospital, creating an infection control risk. In other cases, doctors may make fraudulent claims to be authorised clinical professionals.

Attendees did not conclude that fraud in itself could be generalised to represent a sufficiently serious harm or serious crime to warrant breaches of confidentiality in all cases. Most doubted, for example, that disclosure could be justified to address a case of minor prescription fraud. This suggests it is not the case that any quantity or type of financial harm to public services would carry heavy weighting in a public interest balancing exercise.

Three factors appeared to influence the perceived severity of the fraud, its harm to individuals or to society, and therefore the weighting given to the potential benefit of disclosure. First is the *scale or magnitude of the fraud* being committed, one measurement of this being the quantity of financial loss. This is supported by the definition of serious crime given above in the *Confidentiality: NHS Code of Practice*. An important detail is whether, to determine a severe fraud, magnitude would need to be a feature of a single instance of fraud or could be the sum total of fraud across a system. If the latter, the routine use of NHS data to tackle tax or benefit fraud might carry a heavy weighting in the public interest balancing exercise. Two points, however, resist the interpretation. One attendee noted that generally addressing fraud or tax evasion to improve the amount of funds in the public purse is something that can be achieved just as effectively, if not more effectively, through other policy means. This might make it difficult to argue that the use of NHS data for this purpose is sufficiently necessary. The second is that the concept of the public interest test is rooted in justifications of data disclosure in particular instances of the public interest. The application of a very general public interest might constitute a weaker reason.

The second factor which altered attendees' perceptions of the severity of fraud is the *kind of criminal actor involved*. Some attendees were sympathetic to the argument that organised crime presented a qualitatively different situation and that the weighting of the benefit was increased if disclosure was used to address this type of criminal activity. This sympathy may stem from the supposed scale of the particular fraud, as well as an assessment that organised crime is a destabilising structural problem. One attendee noted that organised crime would represent the kind of misuse of the system which would defeat obligations of confidentiality owed in the first place.

14. Confidentiality: NHS Code of Practice Supplementary Guidance: Public Interest Disclosures. p.9

15. Confidentiality: NHS Code of Practice 2003. p.35

16. The case studies provided by the Home Office are also relevant to this discussion, but as the Home Office provided their information after the workshop, attendees did not discuss the department's position.

The third factor is the *relevance to protecting the NHS*. Many attendees, although not all, were more inclined to give more weight to the benefit of using PDD for tackling fraud in the NHS. This could be for several reasons. NHS data is the only data that can be used to address fraud in the NHS, so this meets the necessity criteria. Heavier weight also might be given to using data in ways relating to purposes for which the data was given in the first place. Patients provide information to the NHS because they are seeking healthcare from the system, so have a greater interest in this system being protected.

The Home Office suggested a principal benefit to the individual whose data was disclosed would be the *regularisation of status.* While accepting that this might entail unwelcome outcomes for individuals who were subsequently forced to leave the country, officials stated it could also lead to the important benefit that individuals were able to enjoy a status that enabled them to become full members of society. If the individual did not benefit from the disclosure of information, the Home Office's view was that society benefitted from the protection of public services, including housing and welfare provision, from being exploited. As noted above, workshop attendees were sceptical about the weight carried by very generalised references to the protection of public services. They were also largely unconvinced that tracing individuals whose only crime was being in the country unlawfully presents enough of a harm to other individuals or society to merit a heavy weighting in the balancing test. However, in specific cases in which individuals are known to be a particular risk to others or vulnerable themselves, they recognised the benefit was likely to be much more substantial, given the widespread acceptance that disclosures may be justified to prevent imminent physical harm. The weight of the individual's interest in status being regularised may need to be determined.

Harms

This section discusses the potentially relevant harms when undertaking a public interest test for using NHS PDD.

The importance of maintaining trust within the doctor-patient relationship and between the public and the health service more generally was a central theme for all attendees in relation to the discussion of harms. Although it is important for all public organisations to be able to marshal trust and accountability, attendees implied they considered high levels of trust to be a primary feature that distinguishes the NHS from other public bodies.

Trust was recognised as central to the health service for multiple reasons. Ethically, it relates to the concept of individual autonomy and patient-centredness on which good medical care is increasingly based. Clinically, trust is important so that individuals are not deterred from seeking healthcare. The value of confidentiality goes beyond actually existing obligations of confidentiality: one attendee remarked that even if a duty of confidence has not actually been engaged through the commencement of a specific doctor-patient relationship, it serves an individual's interest to know that, were they to need such services, relations of confidence are in place and institutionally protected. If trust distinguishes the NHS from other public systems, activities which make it less distinguishable from other parts of the state and its functions, such as policing and surveillance, entail significant costs. Attendees therefore concluded that the undermining of trust is itself a potential harm that should be given heavy weighting in any balancing test.

Attendees highlighted specific harms that might follow if trust is undermined. First is the physical or mental harm individuals might suffer if they are deterred from seeking medical treatment because they have concerns about how their information might be used. These arguments have been raised in relation to disclosures of PDD to the Home Office for the purposes of tracing individuals who lost contact with immigration services.

A second potential harm is the wider detrimental impact on public health if individuals with a disease or infectious condition do not seek healthcare because of concerns their information might be passed on to law enforcement. There is a potential additional impact on health inequalities if certain individuals who are often already socially and economically vulnerable are deterred from seeking care. An increased expectation that information might be shared could also lead members of the public more generally to provide less information in their interactions with clinical professionals. This degradation of the medical record might then lead to difficulties for clinicians in treating patients. In this sense, disclosures of information may contribute to reducing the effectiveness of the NHS.

A final harm is the impact on the professional life of health service workers if the relationship of trust is no longer held in high regard. Some workers might be ambivalent about a closer association with other state functions, but others might feel a conflict with their medical oaths. As one attendee noted, since institutional systems can never be entirely error free, there are likely to be cases where

relations of confidence are broken for insufficient reasons. In this case, even if the information disclosure is made in compliance with an organisational decision, medical professionals are potentially placed in the role of wronging their patients, which could impact their ethical standing.

Although attendees recognised and agreed that confidential information can be used to support law enforcement, it was also clear that they were opposed to the health service becoming incorporated more routinely into the state's policing and surveillance functions. They considered that this threatened the 'special' status of the NHS. A public interest assessment might need to consider to what extent a specific disclosure of data could be interpreted as, and would actually be, a move towards the routinisation of confidential information for law enforcement purposes and the incorporation of the NHS as a public body into other state functions.

Summarising Weightings

Those undertaking a public interest balancing exercise must identify the relevant factors in a potential data disclosure and weigh them carefully to judge whether there is a convincing case in favour of disclosure or maintaining confidentiality.

Certain aspects seemed to affect the weight of proposed benefits of NHS data disclosure in the eyes of attendees. These were: the scale of a specific crime, the nature of its perpetrator, and whether the use of the data is rationally connected to the purposes for which the information was collected i.e. the functioning of the NHS system. Another criterion implied by the discussion was how obviously the proportionality test is satisfied. To be clear, all data disclosures must meet this, but the costs of breaching confidentiality where the information is of less utility, or where other perfectly practicable and equally effective sources of information are available, are likely to balance more heavily against benefits. When multiple data sources are employed to corroborate information, there is not always a simple causal link between the disclosure of a particular piece of data from a source such as the NHS and the outcome. Evidence of effectiveness may therefore need to be considered in broader terms. But it might still be the case that where information is necessary for corroboration, the usage carries greater weight than where it is only helpful. Finally, it would also be relevant to consider how patient expectations align with potential uses of PDD between government agencies, given the emphasis on respecting patient wishes in the health system.

Attendees did not assess what might give greater or lesser weight on the harms side of the equation. This is likely because they were mostly working on the basis of confidentiality being the default assumption against which the burden of proof lay with those advocating the benefits of disclosure.

Process, Justification and Accountability

Attendees thought the institutional procedures through which public interest judgments are made are important and require greater consideration.

The consensus was that such decisions should be able to be scrutinised. The arguments for this were threefold. First, on a normative level, the accountability of public bodies is important in democratic society. People have a right to know how their information is used. The latter point is particularly relevant given the emphasis on respect for the patient. Second, publicly accessible information on the justifiability of decisions, and perhaps some way of appealing those decisions or justifications, is likely to help promote public trust in the organisations disclosing and receiving information. Third, transparency is functionally important. To be able to advise patients on how their information may be used, healthcare professionals need to understand how and why data disclosures are made. The provision of accurate advice to communities and individuals could also help reduce the deterrent effect that has been identified as one of the key harms of data disclosures.

There was recognition that there is a limit to the degree of transparency that is suitable or appropriate. Organisations expressed the view that making detailed information available on specific cases would seriously undermine the effectiveness of their operations by aiding those seeking to evade them. They were reasonably supportive of general principles and processes becoming more transparent. All organisations stressed that their own internal procedures were robust, supported by legislative gateways, written agreements and information governance toolkits, and that processes and decisions were properly recorded on systems.

Attendees discussed several potential avenues for developing greater trust in the data sharing processes between the NHS and other government organisations. The first important factor is awareness of who makes decisions on the public interest and the competence and independence

of this person or persons. It was felt that some training in a standardised process for balancing interests could be useful, and that relevant professionals should be engaged who possess adequate knowledge of different benefits and harms. Several attendees favoured the idea of an advisory body independent of the data disclosing organisation or data recipient, which could be reasonably impartial with respect to short-term political preferences.

The second factor is the clarity and transparency of rules and practices. Transparency operates along a spectrum, the two ends of which might be conceived as mere knowledge that formalised processes exist and knowing the full justification behind actual decisions. An important consideration for formalising process is also the appropriateness of the channels through which information is requested. Specifically, some attendees were critical of information being sought directly from administrative staff at GP surgeries. Evidence that standardised practices exist, it was felt, should be visible. Attendees also emphasised the importance of record-keeping about what, how and why data disclosures had been made, so that such information could be made available for public consumption if necessary.

In summary, most attendees concluded that processes should be formalised and some information on processes and decisions made available to healthcare professionals and the wider public. Government agencies stressed robustness of the governance structures in place around data disclosure agreements, and it is likely that in many cases an appropriate degree of internal regulation already exists. The perception that judgments might be made carelessly, however, or only taking some organisational priorities into consideration and without due regard to the multiple interests at stake, is a significant source of mistrust. Confidence in the process through knowledge of the safeguards that agencies have in place would be welcome.

Conclusion

Confidentiality

Contributors to this report did not reach a consensus position on whether PDD is confidential information, although a majority expressed the view that it should be treated as confidential in all cases. The justifications for this referenced the lack of distinctions made between demographic and clinical information in legislative provisions and professional guidance codes, the difficulty of explaining distinctions to patients, and the universality of the doctor-patient duty of confidentiality in the health system.

This report recommends, therefore, that for the present all PDD is to be considered confidential and to require the public interest justification on a case-by-case basis.

However, given that a substantial number of workshop attendees put forward views that allowed that there are circumstances in which PDD might not be confidential, and a small number disputed the sensitivity of the information itself, there is good reason to continue to nuance the concept of confidentiality.

First, to clarify and precisely identify exactly which pieces of information and which contexts are involved in assessing confidentiality, it may be helpful to typologize data attributes and data contexts. PDD is a collective term, as is 'the health system'. To move beyond a blanket assessment that PDD is (or is not) always confidential in the health system, it would be necessary to discern contexts at a more granular level. Second, further work to assess patients' expectations with regard to the confidentiality of their PDD would enable an ongoing dialogue around what is reasonable and support greater public understanding of information usage. Some studies have added to the growing body of information on patients' expectations of the use of their data, but an in-depth investigation specifically focusing on the questions addressed in this report may advance this particular area.

Public Interest Test

Those undertaking public interest tests do so within a context of legal principles and social and ethical norms. Having proper regard to these mitigates against the balancing exercise becoming a simple utility calculation and should help prevent reductionist outcomes.

This means placing benefits and harms within the context of compliance with the law (both its letter and spirit), ensuring publicly funded bodies carry out their functions fairly and impartially and act 'reasonably' in accordance with public duties. It is important to have certainty that data disclosures are made for legitimate purposes, that the objective is sufficiently important, the measure effective, and that a less intrusive measure could not reasonably have been used. It also means having regard for what the public reasonably expects as well as the responsibility of public bodies towards protecting minority interests. Since this report concerns the use of health system PDD, highly relevant are patient values, wishes and choices, which means recognising that the reasons for

breaching confidentiality must be strong and could be viewed as such, and the medical ethics and professional standards that underpin good healthcare.

Factors potentially relevant in supporting disclosure (benefits)

- Preventing physical or mental harm to individuals.
    - Data subject is vulnerable or at risk; or
    - Data subject is a known risk to other individuals.
- Protecting public services from crimes such as fraud and immigration offences.
    - Effective protection of public services.
    - Effective management of the public purse.
- Improving the functionality of public services e.g. regularising immigration status, less intrusive management of the tax system.

According to attendees, these benefits would not all merit the same weight in a public interest balancing exercise, and the weight granted to a factor will depend on further details.

This report recommends the following criteria give heavier weighting to a factor for disclosure:

- An injury to individuals is imminent and certain.
- In the case of other injuries:
    - The scale of a particular instance of injury is large e.g. large-scale fraud.
    - The nature and intention of the perpetrator is especially malign e.g. organised crime.
    - The injury is committed against the NHS system.
- Disclosure more conclusively meets the proportionality test e.g. more necessary, more effective and strikes a clearer balance between individual rights and the public interest.
- Disclosure obviously supports what the individual thinks is in their interest.

This report recommends the following criteria give lighter weighting to a factor for disclosure:

- Injury is identifiable only in very general, uncertain or indirect terms.
- Data usage less conclusively meets the proportionality test e.g. demonstrates lower degree of necessity and effectiveness and strikes a weaker balance between individual rights and the public interest.

Factors potentially relevant in supporting non-disclosure (harms)

- Trust in the NHS system might be undermined.
- Risk that people will be deterred from seeking care, reducing the ability of the health system to carry out its core purposes.
- Risk to public health if individuals do not seek care.
- Ethical standing of medical professionals might be compromised.
- Risk that the health system becomes incorporated, or seen to be incorporated, more routinely into the other functions of the state.

Criteria which might add or reduce the weight of these factors were not discussed among attendees.

Further work to deduce what patients expect with regard to uses of PDD could be helpful. For example, it could identify to what extent trust in the NHS would be undermined in different circumstances, or whether a use of data would be viewed as too much of an incorporation of the NHS into other state functions.

Process, transparency and accountability

How to improve trust in public interest assessment procedures should be considered. For those who are more sceptical of the appropriateness of data disclosures being made to government agencies, a better understanding of how decisions are made and assurance that they are made carefully and with consideration of the complexity of the subject may provide some reassurance. For medical professionals and those working in the health system, some knowledge of process would enable them to provide informed advice to patients. Finally, for the organisations themselves, the ability and willingness to demonstrate robust processes can be a marker of trustworthiness, supporting the public to have confidence in the operations of public bodies. This must be balanced, however, against the need for transparency not to interfere negatively with those operations.

To improve confidence in the process, attention should be paid to who makes decisions on whether a data disclosure constitutes a public interest, the competence and skills of those making such decisions, their ability to be impartial and fair, and clarity of the rules that are followed.

Attendee list

Matt Bacon
Director of Communications. NHS Digital

Dr Joanne Bailey
National Data Guardian Panel

Paul Buckley
Director of Strategy and Policy. General Medical Council

Dame Fiona Caldicott
National Data Guardian

Dr Tony Calland
Chair. Confidentiality Advisory Group

Dr Vicky Chico
Data Policy Advisor. Health Research Authority

John Chisholm
Chair. BMA Medical Ethics Committee

Professor Carol Dezateux,
Academy of Medical Sciences

Dr Arjun Dhillon
Caldicott Guardian. NHS Digital

Susan Frith
Chief Executive. NHS Counter Fraud Authority

Dr Tom Fowler
Deputy Chief Scientist, Director of Public Health and Caldicott Guardian. Genomics England

Cheryl Gowar
Head of Policy. National Aids Trust

Jackie Gray
Executive Director for Information Governance. NHS Digital

Kiersty Griffiths
Head of Strategy and Planning. General Medical Council

Kirsty Irvine
Chair. Independent Group Advising on Release of Data

Lucy Jones
Director of Programmes. Doctors of the World

Marie Langrishe
PDD Workshop Report Editor

Ros Levenson
Chair Academy Patient and Lay Committee. Academy of Medical Royal Colleges

Katy Lindfield
NHSX (Observer)

Professor Carrie MacEwen
Chair. Academy of Medical Royal Colleges

Professor Neil Manson
Senior Lecturer and Admissions Tutor. Lancaster University

Professor Martin Marshall
Chair. Royal College of General Practitioners

Mike Molloy
Head of Data Analytics Team. Risk and Intelligence Service. HMRC

Professor Andrew Morris
Director. Health Data Research UK

Catherine Nicholson
Associate Director of IG & Data Protection Officer. NHS Digital

Professor Michael Parker
Director of the Ethox Centre. University of Oxford

Lee Pope
Department for Digital, Culture, Media and Sport

Hazel Randall
Associate Director of Legal Services. NHS Digital

Owen Richards
Lay Chair, Patient and Carers Partnership Group. Royal College of General Practitioners

Professor Sir Simon Wessely
Royal Society of Medicine

Arthur Whitehead
National Fugitive Lead. National Crime Agency

Sarah Wilkinson
Chief Executive. NHS Digital

Dr James Wilson
National Data Guardian Panel

Academy of Medical Royal Colleges
10 Dallington Street
London
EC1V 0DB
United Kingdom

Telephone: +44 (0)20 7490 6810
Website: aomrc.org.uk

Registered Charity Number:
1056565

© Academy of Medical Royal Colleges 2021