CHAPTER 7

HEALTH DATA, PUBLIC INTEREST, AND SURVEILLANCE FOR NON-HEALTH-RELATED PURPOSES

Mark Taylor and Richard Kirkham

ABSTRACT

A policy of surveillance which interferes with the fundamental right to a private life requires credible justification and a supportive evidence base. The authority for such interference should be clearly detailed in law, overseen by a transparent process and not left to the vagaries of administrative discretion. If a state surveils *those it governs and claims the interference to be in the public interest, then the evidence base on which that claim stands and the operative conception of public interest should be subject to critical examination. Unfortunately, there is an inconsistency in the regulatory burden associated with access to confidential patient information for non-health-related surveillance purposes and access for health-related surveillance or research purposes. This inconsistency represents a systemic weakness to inform or challenge an evidence-based policy of non-health-related surveillance. This inconsistency is unjustified and undermines the qualities recognised to be necessary to maintain a trustworthy confidential public health service. Taking the withdrawn Memorandum of Understanding (MoU) between NHS Digital and the Home Office as a worked example, this chapter demonstrates how the capacity of the law to constrain the arbitrary or unwarranted exercise of power through judicial review is not sufficient to* level the playing field. *The authors recommend 'levelling up' in procedural oversight, and adopting independent mechanisms equivalent*

Ethical Issues in Covert, Security and Surveillance Research
Advances in Research Ethics and Integrity, Volume 8, 93–118

ISSN: 2398-6018/doi:10.1108/S2398-601820210000008008

to those adopted for establishing the operative conceptions of public interest in the context of health research to non-health-related surveillance purposes.

Keywords: Public interest; confidentiality; independent oversight; health-related surveillance; data protection; privacy

INTRODUCTION

This chapter considers the issue of data sharing in the context of health. Notwithstanding the highly sensitive interests involved, health data have long been known to be of public value for the secondary purposes of medical research and health-related surveillance and can have non-health-related uses as well. This variable use of health data has raised the prospect of an equivalent variability in the oversight of data sharing, creating a risk that, in the long-term, public trust in the security of health data might be undermined. This chapter evidences the problem and outlines a solution.

To illustrate the risks, we explore the example of the now withdrawn Memorandum of Understanding (MoU) in the United Kingdom (UK) between NHS Digital and the Home Office[1] to supply the latter with information obtained by the health service. One of the purposes of the data sharing was to enable the Home Office to better locate those suspected of an immigration offence. Here a decision on the 'public interest' in disclosure was taken without exposure to the kind of open debate that is typically associated with governance models applied before data sharing for other purposes. For example, those seeking access to confidential patient information for the purposes of health research, notwithstanding its public value, must normally have a patient's explicit consent or navigate an approvals process with more independent scrutiny and challenge than was applied to the Home Office's non-health-related surveillance purposes. Health-related surveillance may not always be subject to the same intensity of case-by-case review, and here data disclosure under recent Coronavirus notices may be a good example of reduced review standards being applied. Nevertheless, health-related surveillance in the context of health research is typically characterised by a balance being struck between competing public interests (e.g., between confidentiality and public health protection) that has been relatively precisely articulated in legislation following parliamentary debate and informed by independent advice. The deficit in process for non-health-related surveillance increases the risk that a decision on the public interest in disclosure will have shallow roots, run no deeper than institutional and short-term political interest, and will pay insufficient regard for the interests of all those affected.

We suggest that this situation is problematic for a variety of reasons and provide a recommendation for the way forward. The main concern is that the mischief that the law is designed to address is the need to secure the trust of users of health services, by ensuring that health data is only released, lacking an individual's consent, according to an applied standard of the public interest. To make this argument, we adopt the concept of *social legitimacy* and consider the

extent to which current governance arrangements ensure that those subject to governance have reasons to accept the conceptions of public interest applied by decision-makers.

To address the concerns raised in this chapter, we acknowledge that the law in the UK does provide some constraints on arbitrary or unwarranted exercise of power. However, whilst there is some capacity in judicial remedies, its limitations in this context are also laid bare. Given the problems, this chapter concludes with the recommendation that it is necessary to level the playing field between those who would access confidential patient information for the purposes of health surveillance, those who would access the same data for the purposes of non-health-related surveillance, and those who would access it for the purposes of carrying out research to determine the effectiveness and effects of either type of policy. If social legitimacy in the governance framework is to be upheld, then we would recommend levelling up rather than levelling down. At the heart of the solution needs to be either an extension of parliamentary scrutiny or the expansion of the remit of independent advice on patient data.

This chapter takes the following approach. We begin by establishing the current historical and legal basis for the control of health data in the UK. This is followed by a defence of an important normative purpose of legislation in this context and an argument that this is being undermined by practices exemplified by the, now withdrawn, MoU between NHS Digital and the Home Office. Our conclusion is that the withdrawn MoU illustrates the risk of poor legal design, which currently insufficiently allows for oversight and in this instance was reliant on the ad hoc intervention of a Parliamentary select committee to block potentially unlawful practice. A preferable approach which can pre-empt problems before they arise is to strengthen, in the management of patient data, either prospective parliamentary scrutiny or the role of independent advice, as is already the case for health-related research without explicit patient consent.

THE UK LEGAL FRAMEWORK FOR THE USE OF HEALTH DATA

Background and Legal Context

The importance of being able to use health data for health surveillance purposes is longstanding. For instance, when in 1854 John Snow plotted cases of cholera on a map of Soho in London, his work was dependent on data he had gathered from affected households. For health surveillance to maximise its potential to achieve public health benefits through learning and research, it has long been understood that access to confidential health information is often required. For centuries, this practice was not covered by statute, and instead in law was only dealt with tangentially by the common law duty of confidence. This position became politically untenable around the turn of the millennium, when following a series of scandals, such as Alder Hey (Redfern, Keeling, & Powell, 2001), there was a sustained political reaction to using identifiable health data for purposes beyond individual care without individual consent. The subsequent momentum

towards requiring the explicit consent of a patient for the use of confidential patient information for secondary purposes, jeopardised some health surveillance purposes. At this point, Parliament stepped in.

The significance of sensitive health data for medical purposes beyond individual care, including medical research and health-related surveillance, is today recognised by statutory provisions that permit the duty of confidence to be set aside. This body of law, which is detailed below, allows confidential patient information to flow from general practitioners (GPs), hospital doctors, and other healthcare professionals to national bodies otherwise equipped to monitor and respond to public health risks.

Recent years have revealed, however, the increasing significance and use that may be attached to health data for secondary purposes beyond medical research and health-related surveillance. Advances in information processing, the underlying technological capacity to transfer and analyse big data sets, and the changing – increasingly national (rather than local) level – data flows associated with a modern health care service, are creating new opportunities to use confidential patient information to achieve other kinds of public benefit and undertake other kinds of surveillance activity. The previous use by the Home Office of data obtained and generated through the provision of health care to identify immigration offenders is a case in point. This 'growth area' raises several legal dilemmas, as the use of confidential patient data for surveillance unrelated to medical purpose is not systematically subject to the same procedural safeguards as is the case in relation to use of data for medical purposes. The processes and principles that for nearly 20 years have been associated with the use of health data for secondary medical purposes, including surveillance, are not routinely applied in the case of surveillance for non-health-related purposes. This contrast in legal regimes is detailed below.

Health Surveillance Using Health Data

The powers to share health data for surveillance programmes are extensive and operate within a legal framework that can authorise disclosure without individual patient consent when that is in the public interest. Further, such power to disclose data operates through in-built procedural safeguards that require decisions to be determined upon public interest, safeguards which have their roots in parliamentary disquiet over the possibility of unchecked political discretion regarding the proper conception of public interest to apply in this context. For nearly 20 years, those safeguards have been interpreted and applied by a body charged with providing independent advice to decision-makers.

The foundation of this approach is S. 251 of the National Health Service Act 2006 (re-enacting S. 60 of the Health and Social Care Act 2001), which makes provision for the Secretary of State to lay Regulations establishing a lawful basis for the disclosure of confidential health information for medical purposes. These Regulations can make provision for the common law duty of confidence to be set aside and provide a lawful basis for the disclosure of confidential patient information where none might otherwise exist. Such provisions can be made for a range of purposes, including for surveillance purposes. In fact, it was a perceived

risk to the continued viability of cancer registries in England and Wales that motivated, at least in part, the introduction of the Regulations. When debating them, Lord Hunt of Kings Heath quoted correspondence received from Sir Richard Doll and Sir Richard Peto of the Clinical Trials Service:

> It is, we believe, important for the future health of the people in this country that a legislative framework should exist that ensures that public health surveillance and medical research can continue. (625 Parl Deb HL (5th ser.), 2001, cols. 865–866)

The National Health Service Act 2006 itself, as the parent act, describes the parameters of the Regulations that can be made. It does so widely. Medical purposes are broadly defined to mean the purposes of any of:

> (a) preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of health and social care services, and
>
> (b) informing individuals about their physical or mental health or condition, the diagnosis of their condition or their care and treatment. (National Health Service Act 2006, S. 251(12)(a))

The passage of the legislation was accompanied by continued support for a process to facilitate data sharing, but there was disquiet with the proposal that a Whitehall politician should have the ability to set aside the duty of confidence owed by a health professional to a patient for purposes that were not tightly constrained. The fear was that permitted uses might come to undermine the confidentiality of the health service. This was explicitly recognised by Lord Hunt in debates:

> The breadth of the power sought has been the root of concerns expressed in this House. I fully accept that if such a power did not operate with effective safeguards the potential for misuse might well undermine the trust between patients and the NHS. (625 Parl Deb HL (5th ser.), 2001, col. 866)

The same fear was expressed more forcefully by Earl Howe:

> The mere existence of this power, not to mention the exercise of it, will start the rot. Once doctors and nurses have ceased to be the guardians of the most private information that any of us possess, and once that guardianship has been transferred to a politician in Whitehall, you no longer have a system that will command public trust. That is a process that we should not even countenance. (625 625 Parl Deb HL (5th ser.), 2001, cols. 858–859)

To appease such concerns,[2] the solution was the establishment of an independent body, of broad-based membership, to advise on the purposes for which it was appropriate that any Regulations make provision.[3] As Baroness Northover said when introducing the relevant amendment to the Bill:

> This is simply not an area in which it could ever be appropriate to give such wide powers to the Secretary of State. That is why we propose in the amendment to establish a statutory advisory committee to advise and assist the Secretary of State in this matter … which does not have to sit muzzled in the background as an earlier incarnation, proposed in the other place, just might have done. It consists of representatives of patients' groups, clinicians, medical researchers, health service researchers and others. (625 Parl Deb HL (5th ser.), 2001, cols. 409–410)

The body was known as the Patient Information Advisory Group (PIAG). The resulting Regulations were known as the Health Service (Control of Patient Information) Regulations 2002.

Subsequently, PIAG became an authoritative voice in the control structure around data sharing law in health, including recommending on the content and scope of Regulations laid under the Parent Act. With the benefit of PIAG's advice, under Reg. 3 (1), provision was made for the processing of confidential patient information for the surveillance of communicable diseases and other risks to public health:

(a) diagnosing communicable diseases and other risks to public health;
(b) recognising trends in such diseases and risks;
(c) controlling and preventing the spread of such diseases and risks;
(d) monitoring and managing –
  (i) outbreaks of communicable disease;
  (ii) incidents of exposure to communicable disease;
  (iii) the delivery, efficacy, and safety of immunisation programmes;
  (iv) adverse reactions to vaccines and medicines;
  (v) risks of infection acquired from food or the environment (including water supplies);
  (vi) the giving of information to persons about the diagnosis of communicable disease and risks of acquiring such disease (Health Service (Control of Patient Information) Regulations 2002, Reg. 3(1)).

The Health Service (Control of Patient Information) Regulations 2002 thus provided a lawful basis for health care professionals to disclose confidential patient information for the purposes of surveilling communicable disease and other risks to public health. The processing of confidential patient information for such purposes can *only* be undertaken by one of a number of specified bodies (specified in Reg. 3(3)). There are additional controls built into permitted data flows by the Regulations.

Additional Requirements

As well as being limited to a specific range of bodies, any processing under Reg. 3 is subject to the more general requirements of Reg. 7. These include that:

> (2) No person shall process confidential patient information under these Regulations unless he is a health professional or a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional. (Health Service (Control of Patient Information) Regulations 2002, Reg. 7(2)[4]

It is important to note that the Regulations permit processing that would otherwise be unlawful but do not usually require bodies to disclose information for this purpose. There is the possibility for the Secretary of State to require the processing of confidential patient information for specified purposes under Reg. 3(4) but, to the authors' knowledge, the only occasion on which 3(4) has been relied on is in response to the Coronavirus. In 2021, the Secretary of State issued a number of notices under Reg. 3(4) requiring organisations to process confidential patient information in the manner set out in the notice for purposes set out in

Reg. 3(1). This is currently time-limited (at the time of writing to 30 September 2021) and when the Coronavirus notices expire all relevant information should be deleted.[5]

The Health Service (Control of Patient Information) Regulations 2002, therefore, establish a specific legal basis for the disclosure of health data for 'public health' surveillance purposes. This sits within a broader legal landscape. There are other longstanding legal requirements associated with the disclosure of confidential patient information for public health and indeed for other surveillance.

Other Statutory Disclosures: Health Protection

Since the nineteenth century, under several pieces of legislation, there has been a statutory responsibility to notify certain authorities where infectious diseases are concerned. A distinguishing feature of these responsibilities is that they are heavily constrained by legislation in terms of the scope in which they can be applied, for example, The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013. They do not represent the same 'breadth of power' that was a cause for concern in relation to the more expansively defined 'medical purposes' in S. 251 of the National Health Service Act 2006.

Perhaps the leading example is the Health Protection (Notification) Regulations 2010 (see also Health Protection (Notification) (Wales) Regulations 2010), which extends the previous responsibility and now adopts an 'all hazards' approach. There is now a responsibility upon a registered medical practitioner (R) to notify the proper officer of a local authority where they have 'reasonable grounds for suspecting' that a patient (P) has (or has died from):

(a) a notifiable disease;
(b) an infection[6] which, in the view of R, presents or could present significant harm to human health; or has (having) been
(c) contaminated[7] in a manner which, in the view of R, presents or could present significant harm to human health. (Health Protection (Notification) Regulations 2010, Reg. 2(1))[8]

A crucial distinction with the powers as typically exercised under the Health Service (Control of Patient Information) Regulations 2002 is that the Health Protection (Notification) Regulations 2010 power is not discretionary. The disclosure power is a requirement. Where a local authority has been so notified that there is a responsibility upon them to disclose the fact and content of that notification to Public Health England, the proper officer in the local authority in which P usually resides, and also the proper officer in the Port Authority or local authority in which P has disembarked (from ship, hovercraft, aircraft, or international train) if known (Health Protection (Notification) Regulations 2010, Reg. 6). Diagnostic laboratories also have a duty to notify Public Health England if they identify any 'causative agent' listed within sch. 2 of the Regulations or evidence of any infection caused by such an agent (Health Protection (Notification) Regulations 2010, Reg. 4).

What is noticeable about these Regulations, besides the clear description of mandatory data flow, is that the Confidential Patient Information disclosed is to be either of a particularly restricted nature (relating to a finite list of notifiable diseases) (Health Protection (Notification) Regulations 2010, sch. 1) or associated with infection or contamination that could present *significant* harm to human health. If a health professional were to disclose information in circumstances where they had no reasonable grounds to consider there to be a risk of *significant* harm, they would not be able to avoid liability for a breach of a duty of confidence.[9] There is no such restriction on the Health Service (Control of Patient Information) Regulations 2002 (Taylor, 2015).

Unlike the Health Service (Control of Patient Information) Regulations 2002, PIAG did not advise on the Health Protection (Notification) Regulations 2010, but the legal framework of the parent legislation, the Public Health (Control of Disease) Act (1984), provided significant constraint on the scope of potential Regulations. Where Regulations can plough only a narrow furrow, as established by parent legislation debated in Parliament, the concerns associated with the opaque exercise of power in furtherance of a particular political or narrow institutional agenda are blunted; at least that is, if the Parliamentary process is doing its job through effective opposition and robust debate of legislative proposals in both Houses. It is where statute appears to offer a subsequent opportunity for the exercise of unconstrained discretion that a check and balance on a conception of the public interest in disclosure is most valuable. It was the concern attached to the broad sweep of 'medical purpose' that was contained in the relevant provisions of the Health and Social Care Act 2001 (re-enacted as National Health Service Act 2006, S. 251) that motivated calls for an independent voice on the appropriate breadth and operation of subsequent Regulations.

To summarise: where health-related data are concerned, in UK law two key control devices have emerged. First, legislation has been drafted in such a way to restrict the circumstances in which data can be shared. On this point, there is variability in the extent to which Parent legislation restricts the permissible scope of Regulations. In particular, the breadth of 'medical purpose' in the National Health Service Act 2006 is more permissive than other legislation. To tackle this broader discretionary power, however, a second control device has been attached to the process: namely the establishment of an independent gatekeeper to patient data and an advisor on regulatory and policy reform. Within the parameters established by the National Health Service Act 2006, the role of the advisory group can be seen to vary according to the specificity of the data flows anticipated by individual Regulations. In particular, there is a significant distinction in the operation of Reg. 3 – which permits processing *only* as described for purposes related to communicable disease such as coronavirus and other risks to public health – and Reg. 5 – which permits processing for a relatively broad range of purposes.[9] It is Reg. 5 that is most open ended in scope. In relation to the former (Reg. 3), the advice of PIAG was sought on the appropriate wording of the Regulation. In relation to the latter, the advisory group was further invited to advise on the interpretation and application (of Reg. 5) on a case-by-case basis.

Surveillance/Research Distinction

The different approach taken towards surveillance (under Reg. 3) and medical research (under Reg. 5) under the Health Service (Control of Patient Information) Regulations 2002 may be explainable by the extent to which it was considered possible, at the point in time that the Regulations were being debated, to evaluate the mix and significance of private and public interests engaged. With Reg. 3, the purpose of the surveillance, the nature of the data needed, and the relative importance of the public interest served by such surveillance when compared with the public interest in a confidential health care service could all be taken into consideration during parliamentary debate even if specific public health risks, such as COVID-19, were unknown at the time. As a result, Parliament felt able to say – *in the light of independent advice* – that so far as communicable diseases and other risks to public health to be disclosed under Reg. 3 were concerned, the public interest in disclosure trumped the public interest in confidentiality. Parliament did not feel in a position to make the same sweeping statement in relation to *all* medical research potentially supportable under Reg. 5. Here it was felt more appropriate to put in place a process to enable ongoing, granular, independent scrutiny, and advice.

Before support was given to an activity in pursuit of a medical purpose under Reg. 5, the opinion of PIAG would be sought. PIAG was disbanded in 2008 but at that time the Ethics and Confidentiality Committee (ECC) of the National Information Governance Board took over this advisory function (Health and Social Care Act 2008, S. 157). When the NIGB was itself abolished in 2013, then the advisory role of the ECC transferred to a newly established Confidentiality Advisory Group (CAG). CAG, as part of the Health Research Authority (HRA), continues to offer advice on the use of Reg. 5. In fact, CAG's role in relation to individual decisions on the use of Reg. 5 was put on a statutory footing for the first time by the Care Act 2014 (sch. 7(8)). At that time, the authority for decisions on medical research (as opposed to other non-research-related medical purposes) was passed from the Secretary of State to the HRA. The Secretary of State retains responsibility for making decisions in relation to non-research-related medical purposes.

There are three reasons to draw attention to the Reg. 5 requirement for the scrutiny of applications for the disclosure of confidential information by an independent body, made up of a broad representation, extending to include significant lay membership. First, to highlight the process that has been put in place in the health research context, where there would otherwise be a broad discretion to set aside the duty of confidence and permit disclosure of confidential information without independent advice. Second, to recognise that the advisory group (currently CAG) follows a regular and systematic practice of transparent advice on individual cases of disclosure where the Regulations are most open ended. All minutes, recording advice and reasoning, are published. (The relevance of this will become clear shortly.) Third, to distinguish the process that would need to be undertaken – and the safeguards associated with that process – if a researcher wanted access to confidential patient information (without explicit patient consent) in order to challenge the validity of claims being made in support of a particular use of data for surveillance purposes.

Non-health Surveillance Using Health Data

Up to this point, the focus of the chapter has been on the use of confidential health data for health-related purposes, including what might be described as health surveillance. We will argue shortly that the legal structure put in place is broadly robust, consistent with the purposes of the legislative scheme, and normatively defensible. By contrast, the use of health data for non-health surveillance purposes is less satisfactory.

The Health and Social Care Act 2012 established NHS Digital (originally known as the Health and Social Care Information Centre). The Health and Social Care Act 2012 also established a new legal framework for the flow of confidential information within England and Wales. Under the 2012 Act, NHS Digital not only has the power to require confidential patient information, and other information, from health and social care bodies but also has power to disclose data for both health and non-health related purposes. Although the Health and Social Care Act 2012 impacted significantly upon the legal basis and operational flow of much NHS Data, one thing it did not change was the importance of the Health Service (Control of Patient Information) Regulations 2002 for those seeking access to confidential patient information for secondary 'medical purposes' (as defined by the National Health Service Act 2006, S. 251) without patient consent. If data are disclosed by NHS Digital on the basis of Reg. 5 of the Health Service (Control of Patient Information) Regulations 2002, whether for medical research or health-related surveillance purposes, then independent advice is injected into the process by operation of the arrangements described above. Further to this, due to a change in legislation introduced by the Care Act 2014, CAG now also has a role advising NHS Digital directly on its data dissemination policy. This is further discussed below and is additional to CAG's involvement in the processes associated with operation of the Health Service (Control of Patient Information) Regulations 2002. As we will see though, the operation of this advisory role in practice is quite different from the role of CAG in relation to the Health Service (Control of Patient Information) Regulations 2002. The governance model does not operationally provide equivalent intensity of independent scrutiny prior to a disclosure for non-health-related surveillance purposes.[10]

NHS Digital has the power to require information where it is considered 'necessary or expedient' (Health and Social Care Act 2012, S. 259(1)(a)) for the purposes of any of its statutory functions. As a public body, NHS Digital may only disseminate or publish information where it has specific power to do so. Its powers are set out in the Health and Social Care Act 2012 (S. 261, 262). This includes a range of circumstances set out in S. 261(5)(e). The power of disclosure under S. 261(5)(e) does not set aside the common law duty of confidence and so, where no other legal basis is available, disclosure must be in the public interest. NHS Digital is, as the non-executive public body responsible for collecting, processing, and disseminating significant volumes of confidential patient information across the NHS, accountable for ensuring those data flows are not only lawful but also consistent with its own data publication and dissemination policy. NHS Digital is responsible for any operational decision on disclosure and thus

must determine, in cases where disclosure is only lawful if in the public interest, whether the relevant public interest test is satisfied.

As indicated above, in exercising any function of publishing or otherwise disseminating information, NHS Digital must have regard to any advice given to it by the CAG as the committee appointed by the HRA under sch. 7 Para. 8(1) of the Care Act 2014 to give such advice (Health and Social Care Act 2012, S. 262A (as amended)). However, there is no established process – as there is under the Health Service (Control of Patient Information) Regulations 2002 – for NHS Digital to routinely seek advice in relation to dissemination for specific purposes, and this includes in relation to dissemination for non-health-related surveillance. There is facility for issues to be raised unilaterally by the CAG but, in order to do so, it is necessary for the CAG to be aware that there is an issue to raise (Health Research Authority, 2018). In other words, therefore, issues can be raised with the CAG for advice at the discretion of NHS Digital but there is no *requirement* to do so; and even though the CAG can raise an issue with NHS Digital, it is possible it will not do so due to its lack of prior notification.

There are a number of non-health disclosures that have been made by NHS Digital since its establishment. By way of illustration, this chapter considers disclosures made under a now withdrawn MoU with the Home Office. Consideration of this example demonstrates the variability in oversight and independent advice that accompanies disclosure for different purposes. In relation to secondary *medical* purposes, discretion is exercised following *prior* independent advice on the public interest in *permitting* health professionals to disclose, for example, health research (e.g., Health Service (Control of Patient Information) Regulations 2002, Reg. 5) or communicable disease surveillance (e.g., Health Service (Control of Patient Information) Regulations 2002, Reg. 3). In relation to *non-health*-related purposes (e.g., served by disclosure under Health and Social Care Act 2012, S. 261(5)(e)) discretion may be exercised with *no independent advice*[11] or equivalent consultation on the public interests and yet health professionals may be *required* to provide the information that is disclosed. It also demonstrates the imbalance in regulatory burden felt by those who would use patient data for non-health-related surveillance and those who would access the same data for research purposes (including, potentially, research that might challenge the health impacts of the surveillance).

Disclosure to Home Office Under MOU

NHS Digital entered into a MoU for the purpose of processing information requests from the Home Office to NHS Digital to (re)establish contact between the Home Office and immigrants. This included tracing those suspected of immigration offences and where re-contact would enable their removal from the UK. The MoU was published late in 2016 and came into effect on 1 January 2017, although the practice of providing information to the Home Office had been undertaken before that (House of Commons, Health and Social Care Committee, 2018a, pp. 3–4).

The data requested by the Home Office were limited to demographic/administrative details covering name (or change of name), date of birth, gender, address, and the date of NHS registration. It did not include any clinical information or

information relating to the health, care, or treatment of the individual (Gordon, 2017), but NHS Digital processes still, appropriately in our view (although more on this later), treated the information as confidential (House of Commons, Health and Social Care Committee, 2018a).[12] NHS Digital is empowered to disclose confidential information under S. 261(5)(e) where

> […] the disclosure is made in connection with the investigation of a criminal offence (whether or not in the United Kingdom). (Health and Social Care Act 2012, S. 261(5)(e))

In a letter from Noel Gordon (2017), Chair of NHS Digital, to Dr Sarah Wollaston, Chair of the Health and Social Care Committee, NHS Digital asserted that it was the understanding of NHS Digital that:

> The s261 gateways do not constrain [NHS Digital] to considering only serious offences or harm to the person.

Thus, although NHS Digital acknowledged that where information is confidential and is to be disclosed under S. 261(5)(e), the duty of confidence in such information must still be considered, it suggested a lower threshold may be applied than for other uses of health data. Here, the distinction with the 2010 Regulations (see also Health Protection (Notification) (Wales) Regulations 2010) discussed above is telling, where it is only where there are grounds to consider there to be a risk of *serious* harm that disclosure is required.

According to the letter to the Health and Social Care Committee, the policy of NHS Digital (at the time) was that prior to exercising the power to disclose confidential information under S. 261(5)(e), NHS Digital carried out an assessment which 'weighed the public interest in favour and/or against a disclosure' (Gordon, 2017) in order to avoid an unjustifiable breach of confidence. It was asserted by NHS Digital that 'a public interest test is carried out in each individual case' (Gordon, 2017). The process by which such a test was carried out appears, however, to have been an entirely internal assessment, opaque, and without the benefit of external or independent advice. This individual case consideration was also apparently carried out in the context of not inconsiderable numbers. The Health and Social Care Committee report on the policy noted that there were 10,275 requests for disclosure across the period 2014–2016 (House of Commons, Health and Social Care Committee, 2018a, p. 6).

In terms of retaining the integrity of the overall legal approach towards handling patient data there are several problematic features to this policy. Fundamentally, our concern is with the systemic failure it demonstrates to require equivalent checks and balances on the operative conception of public interest. The lack of independent contribution to an understanding of how the public interest test might operate was strongly criticised by the Health and Social Care Committee (House of Commons, Health and Social Care Committee, 2018a, pp. 9, 18). Following scrutiny by the Health and Social Care Committee, the MoU between NHS Digital and the Home Office was withdrawn (NHS Digital, 2018c).[13] According to NHS Digital's (2018b) website:

> The Home Office can still request non-medical information to locate an individual where this is in the interests of safeguarding an individual and necessary to protect a person's welfare. Any

> such request would be considered by NHS Digital's Welfare Assessment Panel. As at 31 March 2021, NHS Digital has not released any information to the Home Office on these grounds since the MOU was suspended in May 2018.

On the face of it, this may seem to be a success story. An unduly one-sided interpretation of 'public interest' was course-corrected following parliamentary scrutiny. However, our argument is that the need for the *ex post facto* adjustment of the conditions under which the public interest test was understood to be met illustrates the weakness of the process. It is a weakness that persists for so long as decisions on disclosure for non-health surveillance can be made without robust, open, and independent, scrutiny prior to a decision on disclosure being made. The situation is illustrative of the varying intensity of independent challenges to a conception of public interest across the context of health- and non-health-related surveillance due to systemic inconsistencies in review processes across the two contexts.

PROTECTING THE SOCIAL LEGITIMACY OF HEALTH DATA SHARING THROUGH INSTITUTIONAL DESIGN

The example of the MoU and the discussion around health research and surveillance illustrates the potential for the sharing of health data to be managed through very different processes and according to the application of variable, and unevenly applied, law and principle. Of particular concern, is that this example illustrates that in relation to *non-health* surveillance, there is the potential for wide-ranging and discretionary release of confidential information on the basis of an internal assessment of 'public interest' without independent input or review; at least, not prior to a disclosure decision. There is, of course, the possibility of recourse to the courts after sharing, and we consider this further below.

One way to defend a more 'relaxed' policy towards the sharing of health data for the purposes of non-health-related surveillance might be to argue that the data that are being shared, such as basic demographic information about the individual, are not health data for the purposes of the law – and hence not covered by the duty of confidence. To be clear, NHS Digital did state in their evidence to the Health and Social Care Committee that it treated the demographic information as confidential (Gordon, 2017). Nevertheless, at the same time, there is a suggestion in the published material that NHS Digital were of the view that they did not *need* to treat the information as confidential. In a letter to Dr Sarah Wollaston (Chair of the Health and Social Care Committee) the Chair of NHS Digital, Noel Gordon (2017), remarked that:

> It should be noted that the [NHS Digital] treats the administrative information as subject to the duty of confidentiality, notwithstanding that [the Department of Health] considers that such purely demographic/administrative information does not attract the duty of confidence.

Can Demographic Information Be Subject to a Duty of Confidence?

There is good reason to consider demographic/administrative information obtained or generated through the delivery of health care to be covered by the

duty of confidence. In *R (W)* v. *Sec'y of State for Health* (2016), the Court of Appeal found even data that 'falls at the least intrusive end of the spectrum of medical information' may be 'private' (p. 707 [27]). When deciding whether privacy rights are engaged it is necessary to have regard to the 'reasonable expectations' of the subject of the data in question (*Campbell* v. *MGN Ltd.*, 2004). In *R (W)* v. *Sec'y of State for Health* (2016), the Court noted the tendency in all authoritative guidance published to

> […] 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. The documents have been drafted in expansive terms so as to reflect the reasonable expectations of patients that all of their data will be treated as private and confidential. These publicly available documents inform the expectations of patients being treated in the NHS. (p. 710 [39])

This is consistent with other developments in law which support taking *all* factors into account as part of a broader contextual consideration of whether a reasonable expectation of privacy attaches to the use and disclosure of information in all the circumstances. This points against taking any single factor as determinative, including whether data are purely demographic, even if – such as an individual's name – it is already in the public domain. As Lord Nicholls put it in *OBG Ltd.* v. *Allan* (2008):

> As the law has developed breach of confidence, or misuse of confidential information, now covers two distinct causes of action, protecting two different interests: privacy, and secret ("confidential") information …. In some instances information may be in the public domain, and not qualify for protection as confidential, and yet qualify for protection on the grounds of privacy. (p. 72 [255])

Where the courts find that an individual has a reasonable expectation of privacy, taking *all* circumstances into account – including expectations attached specifically to the health care context, then duties will follow even if the information is entirely demographic or administrative and has no clinical detail attached. This may be considered necessary if public trust in the confidentiality of the information provided to a health service is to be protected.

Legislative Purpose and (Social) Legitimacy

If the above argument is correct, then the disclosure of demographic data needs to be considered through the same legal regimes that deal with other categories of health data. On the detail of those legal regimes, evidently Parliament possesses the legal authority to enable discretionary disclosure for the purposes it sees fit. Even so, both a legal and a normative claim can be made about the principles of law that should underpin the design of the processes that manage the control of the sharing of health data. First, processes that manage health data should continue to respect the concerns that motivated Parliamentary debate of S. 251 of the National Health Service Act 2006 (originally enacted as S. 60 of the Health and Social Care Act 2001) and the subsequent Health Service (Control of Patient Information) Regulations 2002. This means that where there is a broad discretion to disclose for purposes beyond individual care, it is necessary to design institutions for health data sharing that will protect public confidence in a confidential

healthcare system. In relation to the processes attached to Regulations laid under S. 251, it was accepted that there needs to be a check on the conception of public interest employed to ensure that it does not slip the moorings of public trust. Whilst the Health and Social Care Act 2012 has established new reasons, and powers through which, to share health data, it does not adjust the importance of preserving public trust as an underpinning purpose of this area of law. If anything, it reiterates that purpose, with NHS Digital being placed under a duty, under S. 253(1) (ca) of the Health and Social Care Act 2012, to have regard to 'the need to respect and promote the privacy of recipients of health services'.

Additionally, there is a deeper normative claim to be made in favour of incorporating a strong public interest element into the legal system where individual rights and collective interests overlap, as they clearly do with health data. This concerns the importance of promoting and protecting the social legitimacy of a process that permits confidential patient information to be used for purposes beyond individual care. As Curtin and Meijer (2006) remark, legitimacy, as a concept, has been variously defined and described:

> First of all purely formal (legal) legitimacy in the sense of the manner in which a particular structure of authority was constituted and acts according to accepted legal rules and procedures. Although many political scientists and lawyers focus on formal legitimacy, some stress the primordial importance of what is termed social (empirical) legitimacy. Social legitimacy refers to the affective loyalty of those who are bound by it, on the basis of deep common interest and/or strong sense of shared identity. (p. 112)

Here it is the latter sense of legitimacy that is considered: social (empirical) legitimacy. We are associating the concept of social legitimacy with 'the capacity of the system to engender and maintain the belief that the existing political institutions are the most appropriate ones for the society' (Lipset, 1981). This approach mirrors thicker accounts of procedural fairness which strive not only to secure in decision-making processes what is formally necessary for lawful public authority, but additionally integrate within them either effective opportunities for participation (Mashaw, 1985) or safeguards which protect the regulated communities involved (Rosanvallon, 2011).

Ultimately, what drives shifts and re-designs to a decision-making process is the need to maintain qualities 'that provide arguments for the acceptability of its decisions' (Mashaw, 1983, p. 24; see also Taylor & Whitton, 2020). This may be a political decision but it is not just the backdrop to the Health Service (Control of Patient Information) Regulations 2002 that suggests that the social legitimacy of the public use of health data should not be taken for granted. In her foreword to the 2016 *Review of Data Security, Consent and Opt-outs* Dame Fiona Caldicott, National Data Guardian for Health and Social Care (2016), remarked that:

> People should be assured that those involved in their care, and in running and improving services, are using such information appropriately and only when absolutely necessary. Unfortunately, trust in the use of personal confidential data has been eroded and steps need to be taken to demonstrated trustworthiness and ensure that the public can have confidence in the system. (p. 2)

This statement was made even before the media reports were released of NHS patient data being handed to the Home Office in an 'immigration crackdown'

(Forster, 2017). The central contention of this chapter is that institutional design of a process that incorporates transparent and open debate of the relative merits of disclosure for surveillance purposes *prior* to a decision being taken is better suited to form a conception of public interest that will meet the demands of social legitimacy. It will promote the principle that data are only released under conditions where this is *acceptable* to those whose data are being used.[14] This is less likely to be achieved through reliance upon the courts to intervene after the fact.

THE LAW AND JUDICIAL CONTROL

One response to demands for social legitimacy and securing the integrity of patient data might be to argue that the strength of the law that surrounds administrative discretion in this area is sufficient to prevent abuse. Indeed, the grounds of administrative law (e.g., *Council of Civil Serv. Unions* v. *Minister for the Civil Serv.*, 1985) have gradually evolved over the years to the point where it is widely accepted that a series of good administration standards are expected of decision-makers, albeit the exact parameters of those standards are a matter of some contention and highly context-specific in application. However, on a number of levels, the saga of the MoU and NHS Digital's subsequent decision making cautions against assuming that by themselves legal safeguards are, or could be, sufficient.

Room for Conflicting Legislative Purposes to Broaden the Use of Disclosure Powers

A first shortfall in the protective value of judicial review is that the lack of specificity within legislation that confers discretionary power can, without further checks and balances, reduce the scope for judicial scrutiny of administrative decision making. To address this problem, a basic test of administrative power is that even if a body possesses a broad power, it needs to be conducted in accordance with the purposes of legislation (*Roberts* v. *Hopwood*, 1925). On this point, the Health and Social Care Act 2012 (S. 261(5)) clearly envisages that NHS Digital has the power to release information for non-health purposes in the following circumstances:

> (a) the information has previously been lawfully disclosed to the public,
>
> (b) the disclosure is made in accordance with any court order,
>
> (c) the disclosure is necessary or expedient for the purposes of protecting the welfare of any individual,
>
> (d) the disclosure is made to any person in circumstances where it is necessary or expedient for the person to have the information for the purpose of exercising functions of that person conferred under or by virtue of any provision of this or any other Act,
>
> (e) the disclosure is made in connection with the investigation of a criminal offence (whether or not in the United Kingdom), or
>
> (f) the disclosure is made for the purpose of criminal proceedings (whether or not in the United Kingdom).

Even where the legislator provides a purpose for discretionary action, however, in a context where strong individual interests are impacted, that power is constrained by a further limiting principle of administrative law, that of 'legality'.

> Fundamental rights cannot be overridden by general or ambiguous words. This is because there is too great a risk that the full implications of their unqualified meaning may have passed unnoticed in the democratic process. In the absence of express language or necessary implication to the contrary, the courts therefore presume that even the most general words were intended to be subject to the basic rights of the individual. (*R* v. *Sec'y of State for the Home Dep't, Ex parte Simms*, 2000, p. 131)

The test of legality has become an increasingly powerful tool within the judicial armoury when interpreting the scope of primary legislation and case law has confirmed that this obligation for clarity in legislation for rights-infringing powers goes beyond those rights that are squarely captured by Convention rights.[15] With regard to S. 261(5), some of the listed circumstances are specific and would appear to meet the test of legality but it is at the very least arguable that, in their specificity, none of these criteria unambiguously sanction a *general* policy of releasing a whole class of data, as opposed to specifically individualised data requests as might be necessary, for instance, to pursue criminal proceedings. The closest we get to a general power to disclose patient data is contained in S. 261(5)(d), but this section appears to possess all the ambiguity of open discretion that the 'legality' test is designed to block.

The argument of legality, therefore, is a powerful weapon against an unchecked general discretionary power to share patient data. Our concern, however, is that there is sufficient specificity to allow for a certain degree of discretionary disclosure in individual cases in circumstances where the legislation is otherwise silent on any subsidiary checks that might be used to control or limit that discretion's operation.

Limits to the Ability to Scrutinise the Merits of Individual Decisions

A second shortfall with relying upon legal rectification of errors in the disclosure of information is that the room for the courts to scrutinise individual decisions is narrow. Through the common law, when considering whether a public body was justified in introducing a policy, such as a policy of surveillance, the courts may be invited to consider the quality of the reasoning or evidence underlying or supporting the decision:

> Courts, under judicial review, rather than appeal, will not normally interfere with a public authority's assessment of the evidence or facts of a case. However, interference has been permitted where the decision is unsupported by substantial evidence, sometimes called a perverse decision. Recently the courts have been prepared also to intervene where there has been a misdirection, disregard or mistake of a material fact. (Jowell, 2015, pp. 51–52)

Nevertheless, albeit a limited form of rationality review of the substance of decisions may be available, where the duties owed towards affected individuals are left undetailed in legislation the intensity of review will be light. Further, even if the process by which such standards is made is left underdeveloped, the common law only partially fills the void. Ideally, if an *individual* is to be deprived of

a benefit, such as control over their personal data, then as well as notice of the decision they should have opportunity to make representation and have individualised reasons provided. The 2012 Act, though, does not require NHS Digital to notify individuals that their health data have been shared or to provide reasons for the sharing of information. Plausibly, the strength of interest involved might establish a ground for arguing that common law procedural fairness requires some input of individuals before decisions are made (*McInnes* v. *Onslow-Fane*, 1978), or that reasons should be provided (*R* v. *Sec'y of State for the Home Dep't, Ex parte Doody*, 1994). Along these lines, one of us has previously argued that a respect for human rights will require an organisation to *consult* prior to adopting a policy that impacts negatively upon an individual's fundamental rights and freedoms (Grace & Taylor, 2013). This may be as close as a court would be willing to get to requiring the kind of input into a decision-making process that has taken place in the context of health surveillance and in the exercise of discretion in relation to health research. It is also highly likely that the intensity of the scrutiny of the substance of the decision would be restricted by the deferential nature of the *Wednesbury* reasonableness test, particularly where a powerful competing public interest, such as security, can be appealed to.

Stronger tests through which to challenge individual decisions are available under the Human Rights Act 1998. Under the Human Rights Act 1998 decisions must be compatible with Convention rights and tested against a more intensive test of proportionality review. The most obvious human right that surveillance will engage is the right to respect for a private and family life. The Human Rights Act 1998 makes it unlawful for a public authority to act in a way that is incompatible with the right to respect for private and family life, home and correspondence, protected by art. 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, or ECHR). Under Art. 8(2):

> There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well being of the country, for the prevention of disorder or crime, for the protection of health and morals, or for the protection of the rights and freedoms of others. (Convention for the Protection of Human Rights and Fundamental Freedoms, 1950)

Disclosure of confidential patient information, for the surveillance purposes, will constitute a prima facie interference with Article 8 unless disclosure was authorised by the patient. The Human Rights Act 1998 does then provide an action by which the *necessity* of an interference, even if in pursuit of a legitimate aim, may be challenged.

In the case of *de Freitas* v. *Permanent Sec'y of Ministry of Agric., Fisheries, Lands and Hous.* (1999), the Privy Council considered the meaning of the phrase 'reasonably necessary' and adopted a three-stage test:

> whether: (i) the legislative objective is sufficiently important to justify limiting a fundamental right; (ii) the measures designed to meet the legislative objective are rationally connected to it; and (iii) the means used to impair the right or freedom are no more than is necessary to accomplish the objective. (p. 80, citing *Nyambirai* v. *Nat'l Soc. Sec. Auth,.*, 1996, p. 75)

This test has been subsequently adopted by British Courts when determining if an interference with a convention right is necessary, with recognition that analysis of these three elements introduces questions of proportionality (*Huang* v. *Sec'y of State for the Home Dep't*, 2007; *R (Daly)* v. *Sec'y of State for the Home Dep't*, 2001, p. 547). It is through the concept of necessity, and the associated concept of proportionality, that the courts could subject a policy of surveillance to – what might approach –merit based review:[16] determining whether the objective of the surveillance was 'sufficiently important', whether surveillance was a rational approach to achieving the objective, and whether the interference that the surveillance represents is necessary (read 'proportionate') to achievement of that objective.

Although there is the possibility, through the concept of proportionality, for a closer review of the merits of a decision than would ordinarily be associated with judicial review, there is still classically, a 'margin of appreciation' afforded national authorities when it comes to reasonable disagreement regarding what is understood be 'necessary' (*Handyside* v. *U.K.*, 1976, p. 754). A domestic equivalent, affording the executive a margin of appreciation relative to the court's own assessment, must be understood to operate at least consistently with respect for the separation of powers.[17]

Judicial Review Is a Retrospective Solution Only

A third risk with relying upon judicial oversight is that judicial review is a remedy of last resort. Certainly, judicial review is a potentially powerful process, and the latent prospect of judicial review should discourage arbitrary decision making and encourage a public body to ensure a decision-making process will bring relevant issues into consideration. But, there is now a wealth of literature that demonstrates that it operates very much as a reserve remedial route and is informally set up to filter out many more cases than it filters in (Bondy & Sunkin, 2009). It is, in other words, a process that can provide some assurance as to the quality of decision making in NHS Digital but only an intermittent assurance check, and arguably a disproportionately legal form of assurance at that. For most decision-making processes alternative safeguards are often better equipped either to provide efficient redress or in preventing administrative error before it occurs. More importantly, judicial review is a process that need not promote the social legitimacy discussed earlier, nor challenge the *relative* value attached to the interests of a confidential health care system and identification of immigration offenders.

THE WAY FORWARD: EXPANDING THE REMIT OF THE INDEPENDENT ADVISORY BOARD

The context of state sponsored surveillance of data collected by the health service for the purposes of supporting immigration policy is one that well-illustrates the risks of non-health-related use of health data. This policy demonstrates an embedded inconsistency in the manner in which health data are currently being

managed, which in turn risks undermining the integrity of the system and user confidence in the health sector.

The above section has argued that there are grounds upon which the legality of the use of health data for non-health-related surveillance may be challenged. However, neither the prospect of challenge for unjustified interference with human rights, nor judicial review, are likely to provide the long-term fix to the risks that the former use of the MoU gave rise to. A further solution might be for Regulations to be introduced, or better still the Health and Social Care Act 2012 to be amended, to stipulate more detailed restrictions on the sharing of health data by NHS Digital for non-health-related purposes. Within such legislation, the process of balancing competing interests could be made transparent and consultative, and the relevant factors upon which such balancing exercises are based (such as seriousness of offences for which data are sought) could be outlined.

However, although more guidance on the relevant factors for developing policies on disclosure would be a step forward in terms of clarifying the legal authority of NHS Digital and the lawfulness of such administrative practices as the MoU, it would not address many of our wider concerns. Judicial review would continue to operate as a safeguard, but almost certainly an insufficient one which could only intermittently introduce into the decision-making process the kinds of challenge, independent advice, or transparency that can be offered by the processes associated with a specialised independent advisory body, such as CAG or the National Data Guardian (Health and Social Care (National Data Guardian) Act 2018). To provide this ongoing scrutiny there needs to be an additional process put in place prior to a decision on release of data, either on a case-by-case basis (e.g., Health Service (Control of Patient Information) Regulations 2002, Reg. 5) or before new policies are struck.

The institutional solution of an independent advisory body, or watchdog, is one that has been adopted across governance in circumstances where, for a variety of reasons, an element of independence is seen as necessary to ensure that the decision-making process retains loyalty to the full set of values underpinning the scheme (Vibert, 2007). Independence is promoted as a safeguard needed to establish trust in the use of public power by facilitating a process through which certain exercises of public power can be either blocked or 'fire-alarms' raised as to potentially arbitrary or otherwise undesirable decision making (McCubbins & Schwartz, 1984). Reasons for the advisory body solution might also include the lack of time, knowledge, skill, and possibly inclination of other options (in particular, the courts or Parliament) for performing a monitoring role.

Taking all this together, in the context of considering whether a request for surveillance is justified *prior* to a decision being made, extending the requirement for independent review prior to disclosure would have five clear advantages to relying upon judicial oversight alone:

1. *Method*: A body offering independent advice on public interest prior to a decision being taken can adopt an inquisitorial approach and reflect the results of broad consultation within its advice. It can request evidence on relative effectiveness prior to implementation or alongside implementation as part of

an evaluation of implementation. A court is more constrained by the adversarial nature of the judicial process and the limited range of opportunities it has to instigate independent investigation, revisit a position over time, or request evidence of impact be gathered after its decision.
2. *Skill-set:* Independent advice can draw on a range of relevant expertise to the function on hand, including but not exclusively so, legal expertise. Such input is unlikely to be incorporated into standard judicial review proceedings.
3. *Operability:* A claim for unlawful interference with an individual's interests or rights is subject to an individual's disposable resource (in terms of both time and money) and motivation. An independent body established for the purpose and part of an established process is subject to no such constraint. Independent bodies can also operate in circumstances where the affected individuals may not be well aware of their loss of rights.
4. *Timeliness:* Judicial determination can only follow sometime after a decision has been made – and a policy has been implemented. The harm to public trust and confidence may already be done. Advisory bodies can operate more flexibly both before and after decisions are made.
5. *Challenging:* Those invited to provide independent advice, as opposed to making a decision, on the merits of an issue need not worry – in the same way that a court might – about inappropriately overstepping the separation of powers. Its accountability function is as much one of providing transparency and moral suasion, as it is determining outcomes. Advisory bodies can also operate as 'disrupters', challenging institutional biases.

Many of these advantages are also possessed by Parliamentary select committees but, as in the case of the MoU discussed in this chapter, Parliament is a powerful but generally reactive and randomly triggered safeguard. Parliament can work well for crisis moments in administrative malpractice but is less likely to be effective, or as prompt, as a regular monitor of administrative policy making (Flinders, 2008, pp. 184–189).

CONCLUSION

Decisions taken by those with the authority to interfere with fundamental rights and freedoms *ought* to be based on evidence. For this reason, one might expect a policy of surveillance which interferes with the fundamental right to a private life, to require credible justification and an evidence base. It should also be one that is clearly detailed in law and not left to the vagaries of administrative discretion. If a state surveils those it governs and claims the interference to be in the public interest, then the evidence base on which that claim stands should be subject to critical examination.

This volume explores many aspects of the rapidly changing and evolving surveillance landscape. This chapter has considered just one aspect of this: the regulatory framework relevant to public policy decisions on surveillance, the efficacy of which may be informed by health research in England and Wales. The chapter

has addressed just two questions in this context: (1) Is any inconsistency in regulatory burden associated with access to confidential patient information for non-health-related surveillance purposes and access for health-related surveillance purposes justified? (2) Is any inconsistency in regulatory burden associated with surveillance and the research necessary to inform, or challenge, that policy of surveillance consistent with the promotion of evidence-based decision making?

The suggestion is that the regulatory framework is deficient in this regard: there is an uneven playing field occupied by those seeking access to data for health- or non-health-related surveillance purposes and also policymakers and researchers when it comes to accessing the data needed to evaluate the efficacy of public policy. Unless we are able to independently interrogate the quality of the data on which public policy decisions on surveillance are based, we cannot challenge any justification for a surveillance policy. Further, a failure to allow researchers access to the data under the same conditions as policymakers is a failure to promote evidence-based decisions, as the decision-makers are not readily challenged.

Clinicians see themselves as gatekeepers, fiercely protective of the sensitive data entrusted to them. Without a patient's explicit consent there will be only a very limited range of circumstances under which health professionals will disclose confidential health information for purposes beyond individual care. Health researchers have long complained of the difficulties they face in obtaining confidential health information for research purposes. Besides the legal constraints, there are systems of approval and a culture of caution to be navigated. Where pursuit of statutory purposes involves surveillance of health data, the process by which such data can be lawfully accessed is different from those processes that health researchers must navigate. This results in a different regulatory burden. This is not consistent with promotion of social legitimacy and public trust in a confidential healthcare service.

If society is to be able to challenge the quality of a decision to surveil the population, then there must be independent research access to the data underpinning a decision to surveil. Such access should bear an equivalent regulatory burden to the access for surveillance purposes. Otherwise, we introduce systemic obstruction to access the data necessary to hold government action to account. Put simply, it should not be easier to get the data for surveillance purposes than to get the data to carry out research on the impacts of such surveillance.

NOTES

1. The Home Office is one of the largest government departments in the UK, with a wide range of security-related responsibilities, including border control, immigration, citizenship, policing, prisons, law and order, and tackling terrorism.

2. It should be recognised that the suggestion of a statutory committee did not in fact satisfy Earl Howe, who thought the risk to public confidence by the breadth of the power insufficiently contained. It was enough, however, to enable the Bill to make progress through both Houses.

3. The responsibility to consult the Patient Information Advisory Group (PIAG) was originally contained in S. 61 of the Health and Social Care Act 2001. The responsibility to consult its successor body, the Ethics and Confidentiality Committee (ECC) (as part of the National Information Governance Board (NIGB)) was under S. 252 of the National

Health Service Act 2006 prior to amendment. When the NIGB was abolished, the relevant body to consult became the Care Quality Commission (see Health and Social Care Act 2012, S. 280(5)).

4. For the purposes of Health Service (Control of Patient Information) Regulations 2002, art. 7 ¶ 2, 'health professional' has the same meaning as in S. 69(1) of the Data Protection Act 1998.

5. Coronavirus (COVID-19): Notification to organisation to share information. Department of Health and Social Care. (Last updated 10 February 2021.)

6. Any reference to infection or contamination is 'a reference to infection or contamination which presents or could present significant harm to human health' (Public Health (Control of Disease) Act 1984, S. 45A(2)).

7. Contamination includes radiation (Public Health (Control of Disease) Act 1984, S. 45A(2).

8. The duty in relation to the living is contained within art. 2 (Health Protection (Notification) Regulations 2010). The duty in relation to the dead is within art. 3 (Health Protection (Notification) Regulations 2010)).

9. Subject to art. 7, confidential patient information may be processed for medical purposes in the circumstances set out in the Schedule to these Regulations provided that the processing has been approved –

(a) in the case of medical research, by both the Secretary of State and a research ethics committee, and

(b) in any other case, by the Secretary of State.

10. NHS Digital has an internal committee, established for the purpose of independent advice, known as the committee on Independent Group Advising on the Release of Data (IGARD) (NHS Digital, 2018a). There is no mention in the minutes of IGARD of any request to comment on dissemination in relation to the Home Office for immigration offender tracing. A matter commented upon by the Health and Social Care Committee: 'We also find it disturbing that the matter has not been considered by NHS Digital's own Independent Group Advising on the Release of Data (IGARD)' (House of Commons, Health and Social Care Committee, 2018, p. 23). For NHS Digital's explanation on non-consultation with IGARD, see Health and Social Care Committee (2018, Q116–Q118).

11. NHS Digital hosts an independent advisory board, known as IGARD (Independent Group Advising (NHS Digital) on the Release of Data), but the Health Select Committee found that data sharing with the Home Office under the MoU had not been considered by IGARD. A fact that the Chair of the Committee described as 'disturbing'. House of Commons, Health and Social Care Committee (2018c, January 29).

12. Note that the continued operation of the duty of confidence led the National Data Guardian to comment that NHS Digital may have drawn too much from the fact that S261(5)(e) does not constrain disclosure to only serious offence or harm (House of Commons, Health and Social Care Committee, 2018, p. 14).

13. For discussion of announcement see blog post by Understanding Patient Data (2018).

14. On the difference between acceptable and preferable see Taylor and Taylor (2014). On the significance of acceptability to public interest decision making, see Taylor and Whitton (2020). For an interesting discussion of the significance of public engagement to public interest decision making see Sorbie (2020).

15. This test goes beyond the Human Rights Act 1998. See, for example, the use of the test in *R* v. *Hughes* (2013) and *R (UNISON)* v. *Lord Chancellor (Equal. and Human Rights Comm'n) (Nos. 1 and 2)* (2017).

16. For discussion of the extent to which the intensity of such review may vary in difference ways, according to the exigencies of judicial deference and judicial restraint, see Rivers (2006).

17. For more on why assessment of proportionality must respect separation of powers see Rivers (2006).

REFERENCES

625 Parl Deb HL (5th ser.) (2001) (UK).

Bondy, V., & Sunkin, M. (2009). The dynamics of judicial review litigation: The resolution of public law challenges before final hearing. Retrieved from https://publiclawproject.org.uk/resources/the-dynamics-of-judicial-review-litigation/

Campbell v. *MGN Ltd*. (2004) 2 AC 457 (HL) (appeal taken from Eng.).

Care Act 2014, c. 23 (Eng.).

Convention for the Protection of Human Rights and Fundamental Freedoms. (1950, November 4), 213 U.N.T.S. 221.

Coronavirus (COVID-19). (2020 [updated 2021]). Notification to organisation to share information. Department of Health and Social Care. Retrieved from https://www.gov.uk/government/publications/coronavirus-covid-19-notification-of-data-controllers-to-share-information

Council of Civil Serv. Unions v. *Minister for the Civil Serv*. (1985) AC 374 (HL) (appeal taken from Eng.).

Curtin, D., & Meijer, A. J. (2006). Does transparency strengthen legitimacy? A critical analysis of European Union policy documents. *Information Polity*, *11*(2), 109–122.

Data Protection Act. (1998), c. 29 (Eng.).

de Freitas v. *Permanent Sec'y of Ministry of Agric., Fisheries, Lands and Hous*. (1999) 1 AC 69 (appeal taken from Eastern Caribbean CA).

Flinders, M. (2008). *Delegated governance and the British state: Walking without order*. Oxford: OUP. doi:10.1093/acprof:oso/9780199271603.001.0001

Forster, K. (2017, January 25). NHS patient data handed to Home Office in immigration crackdown. *The Independent*. Retrieved from https://www.independent.co.uk/

Gordon, N. (2017, March 6). Letter to Sarah Wollaston. Publications: Health and Social Care Committee, UK Parliament. Retrieved from https://www.parliament.uk/globalassets/documents/commons-committees/Health/Correspondence/2016-17/Correspondence-Memorandum-Understanding-NHS-Digital-Home-Office-Department-Health-data-sharing.pdf

Grace, J., & Taylor, M. J. (2013). Disclosure of confidential patient information and the duty to consult: The role of the Health and Social Care Information Centre. *Medical Law Review*, *21*(3), 415–447. doi:10.1093/medlaw/fwt013

Handyside v. *U.K., 24 Eur. Ct. H.R. (ser. A)* (1976).

Health and Social Care Act 2001, c. 15 (Eng.).

Health and Social Care Act 2008, c. 14 (Eng.).

The Health Protection (Notification) Regulations 2010, SI 2010/659 (Eng.)

The Health Protection (Notification) (Wales) Regulations 2010 W.S.I. 2010/1546 (W. 144).

The Health Service (Control of Patient Information) Regulations 2002, SI 2002/1438 (Eng.).

Health Research Authority. (2018). CAG advice to NHS Digital. Retrieved from https://www.hra.nhs.uk/about-us/committees-and-services/confidentiality-advisory-group/cag-advice-nhs-digital/

House of Commons, Health and Social Care Committee. (2018a). Memorandum of Understanding on data-sharing between NHS Digital and the Home Office: Fifth report of session 2017–19. Retrieved from https://publications.parliament.uk/

House of Commons, Health and Social Care Committee. (2018b, March 15). Oral evidence: Memorandum of Understanding on data-sharing, HC 677. Retrieved from http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/health-and-social-care-committee/memorandum-of-understanding-on-datasharing-between-nhs-digital-and-the-home-office/oral/80609.html

House of Commons, Health and Social Care Committee. (2018c, January 29). Letter from the Chair of the Committee to the Chief Executive of NHS Digital. Retrieved from https://publications.parliament.uk/pa/cm201719/cmselect/cmhealth/677/67709.htm

Huang v. *Sec'y of State for the Home Dep't* (2007) 2 AC 167 (HL) (appeal taken from Eng.).

Human Rights Act. (1998), c. 42 (Eng.).

Jowell, J. (2015). Proportionality and unreasonableness: Neither merger nor takeover. In H. Wilberg & M. Elliott (Eds.), *The scope and intensity of substantive review: Traversing Taggart's rainbow* (pp. 41–60). London: Hart Publishing.doi:10.5040/9781474202701

Lipset, S. M. (1981). *Political man: The social bases of politics*. Baltimore, MD: Johns Hopkins University Press.

Mashaw, J. L. (1983). Bureaucratic justice: Managing social security disability claims. Retrieved from https://www.jstor.org/stable/j.ctt1dt009d

Mashaw, J. L. (1985). *Due process in the administrative state*. New Haven, CT: Yale University Press.

McCubbins, M. D., & Schwartz, T. (1984). Congressional oversight overlooked: Police patrols versus fire alarms. *American Journal of Political Science*, *28*(1), 165–179. doi:10.2307/2110792

McInnes v. *Onslow-Fane* (1978) 1 WLR 1520 (ChD).

National Data Guardian for Health and Care. (2016). Review of data security, consent and opt-outs. Retrieved from https://www.gov.uk/government/publications/review-of-data-security-consent-and-opt-outs

National Health Service Act 2006, c. 41 (Eng.).

NHS Digital. (2018a). Independent group advising on the release of data. Retrieved from https://digital.nhs.uk/about-nhs-digital/corporate-information-and-documents/independent-group-advising-on-the-release-of-data

NHS Digital. (2018b). National back office for the personal demographics service. Retrieved from https://digital.nhs.uk/services/national-back-office-for-the-personal-demographics-service#home-office-tracing-service

NHS Digital. (2018c). Memorandum of Understanding (MOU) on processing information requests from the Home Office to NHS Digital to be able to trace immigration offenders. Retrieved from https://www.gov.uk/government/publications/information-requests-from-the-home-office-to-nhs-digital

Nyambirai v. *Nat'l Soc. Sec. Auth.* (1996) 1 LRC 64 (SC) (Zim.).

OBG Ltd. v. *Allan* (2008) 1 AC 1 (HL) (appeal taken from Eng.).

Public Health (Control of Disease) Act 1984, c. 22 (Eng.).

R (Daly) v. *Sec'y of State for the Home Dep't* (2001) 2 AC 532 (HL) (appeal taken from Eng.).

R (UNISON) v. Lord Chancellor (Equal. and Human Rights Comm'n) (Nos. 1 and 2) (2017) 3 WLR 409 (SC) (appeal taken from Eng.).

R (W) v. *Sec'y of State for Health* (2016) 1 WLR 698 (CA).

R v. *Hughes* (2013) 1 WLR 2461 (SC) (appeal taken from Eng.).

R v. *Sec'y of State for the Home Dep't*, Ex parte *Doody* (1994) 1 AC 531 (HL) (appeal taken from Eng.).

R v. *Sec'y of State for the Home Dep't*, Ex parte *Simms* (2000) 2 AC 115 (HL) (appeal taken from Eng.).

Redfern, M., Keeling, J. W., & Powell, E. (2001). The Royal Liverpool children's inquiry: Report. Retrieved from https://www.gov.uk/government/publications/the-royal-liverpool-childrens-inquiry-report

The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations (2013), SI 2013/1471 (Eng.).

Rivers J. (2006). Proportionality and variable intensity of review. *Cambridge Law Journal*, *65*(1), 174–207. doi:10.1017/S0008197306007082

Roberts v. *Hopwood* (1925) AC 578 (HL) (appeal taken from Eng.).

Rosanvallon, P. (2011). Democratic legitimacy: Impartiality, reflexivity, proximity. Retrieved from https://www.jstor.org/stable/j.ctt7stdc

Sorbie, A. (2020). Sharing confidential health data for research purposes in the UK: Where are the 'publics' in the public interest?. *Evidence & Policy: A Journal of Research, Debate and Practice*, *16*(2), 249–265. doi:10.1332/174426419X15578209726839

Taylor, M. J. (2015). Legal bases for disclosing confidential patient information for public health: Distinguishing between health protection and health improvement. *Medical Law Review*, *23*(3), 348–374. doi:10.1093/medlaw/fwv018

Taylor, M. J., & Taylor, N. (2014). Health research access to personal confidential data in England and Wales: Assessing any gap in public attitude between preferable and acceptable models of consent. *Life Sciences, Society and Policy*, *10*(15), 1–24. doi:10.1186/s40504-014-0015-6

Taylor, M. J., & Whitton, T. (2020). Public interest, health research and data protection law: Establishing a legitimate trade-off between individual control and research access to health data. *Laws*, *9*(1), 6. doi:10.3390/laws9010006

Understanding Patient Data. (2018). Changes to the Home Office – NHS Digital Memorandum of Understanding. Retrieved from https://understandingpatientdata.org.uk/news/memorandum-understanding-changed

Vibert, F. (2007). *The rise of the unelected: Democracy and the new separation of powers*. New York, NY: Cambridge University Press. doi:10.1017/CBO9780511491160