Medical Law Review, Vol. 0, No. 0, pp. 1–22
doi:10.1093/medlaw/fwx038

USING AND DISCLOSING CONFIDENTIAL PATIENT INFORMATION AND THE ENGLISH COMMON LAW: WHAT ARE THE INFORMATION REQUIREMENTS OF A VALID CONSENT?

VICTORIA CHICO[1,*] AND MARK J. TAYLOR[2]

[1] School of Law, University of Sheffield, Sheffield, S3 7ND, UK
[2] School of Law, University of Sheffield, Sheffield, S3 7ND, UK
*v.chico@sheffield.ac.uk

ABSTRACT

The National Health Service in England and Wales is dependent upon the flow of confidential patient data. In the context of consent to the use of patient health data, insistence on the requirements of an 'informed' consent that are difficult to achieve will drive reliance on alternatives to consent. Here we argue that one can obtain a valid consent to the disclosure of confidential patient data, such that this disclosure would not amount to a breach of the common law duty of confidentiality, having provided less information than would typically be associated with an 'informed consent'. This position protects consent as a practicable legal basis for disclosure from debilitating uncertainty or impracticability and, perhaps counter-intuitively, promotes patient autonomy.

KEYWORDS: Confidentiality, health data, informed consent, real consent, reasonable expectations

I. INTRODUCTION

While a considerable literature has been generated around the subject of consent, there has been relatively little discussion of the informational requirements of a valid consent from the perspective of the common law duty of confidentiality. This is

perhaps surprising. It is no exaggeration to say that the future of the National Health Service, along with other health systems across the world, is dependent upon the flow of confidential data. Confidential patient data[1] must flow not only to support the delivery of individual care. Confidential data must also—at times—flow to enable a health system to operate and to learn: to establish what works, what does not work, what could be done more effectively, efficiently, and safely.

In England and Wales, guidance on legal responsibilities associated with handling confidential patient data will often provide a summary at some point similar to that provided in the 2003 NHS Confidentiality: Code of Practice:

> information that can identify individual patients, must not be used or disclosed for purposes other than healthcare without the individual's explicit consent, some other legal basis, or where there is a robust public interest or legal justification to do so.[2]

The healthcare that is imagined in this guidance is the patient's own. Identifiable patient data may flow to support a patient's own care based on an *implied* consent. Any further use of identifiable patient data requires an *explicit* consent or some other legal justification. This responsibility to obtain explicit patient consent, or alternative legal justification, is attributed to the common law duty of confidentiality.[3] Of course, the law of confidence sits within a broader complex of responsibilities[4] but it is true to say that it is principally the common law duty, interpreted in the context of the Human Rights Act 1998 that is understood to drive the responsibility to obtain patient consent for the disclosure of confidential data.[5]

---

1 We refer to patient data, rather than patient information, to avoid discussing the *information* to be provided in relation to use or disclosure of *information*. Otherwise, for the purposes of this article, the terms data and information should be considered interchangeable.

2 Department of Health *Confidentiality: NHS Code of Practice* (November 2003) 7. See also GMC *Confidentiality* (2009) 6.

3 The Data Protection Act 1998 (DPA) itself imposes no such requirement. Paragraph 8 of sch 3 of the DPA provides an alternative legal basis to consent for a data controller when processing for medical purposes. There is an argument that a proper understanding of schs 2 and 3 of the DPA would prioritise consent as 'first among equals' and, as per the Human Rights Act 1998, any failure to process on the basis of consent would require justification as necessary and proportionate, in accordance with law, and in pursuit of a legitimate aim. See, for example, D Beyleveld, 'Data Protection and Genetics: Medical Research and the Public Good' (2007) 18 King's Law Journal 275, 284–85. However, that does not appear to be the current advice of the Information Commissioner's Office (ICO). See, for example, the ICO response to GMC Consultation on Confidentiality Guidance. In particular, in response to question 8: 'If it is anticipated that the disclosure has a legal basis to take place anyway, regardless of consent, then for the purposes of the DPA another schedule condition should be applied and consent not sought - patients should simply be clearly informed that the disclosure will take place, to whom and why'. <https://ico.org.uk/media/about-the-ico/consultation-responses/2015/1043273/ico-response-to-gmc-confidentiality-guidance-consultation.pdf> accessed December 2016.

4 In England and Wales, the use and disclosure of confidential patient information is subject to several legal governance mechanisms. These include, but are not limited to: the Data Protection Act 1998, the Human Rights Act 1998, the National Health Service Act 2006, including Regulations laid under s 251, the Health and Social Care Act 2012, the common law of confidentiality, and the tort of misuse of private information.

5 See Department of Health (n 2) paras 33 and 41.

The relative paucity of legal discussion of the informational requirements of a valid consent might be attributable to many of the leading cases on breach of confidence focusing on justifications other than consent.[6] Furthermore, there may be an assumption that the law here simply mimics the requirements of a valid consent in other areas.[7] However, because the legal informational requirements of a valid consent are not uniform across different areas of law, there needs to be some discussion of the most appropriate approach to informing a consent in the law of confidence. The value of doing so can be illustrated with reference to current and upcoming issues.

In October 2016, the Association for Clinical Genetic Science (ACGS) and the Public Health Genomics (PHG) Foundation collaborated in delivery of an evidence session for the National Data Guardian (NDG). The session sought to engage the assistance of the NDG in addressing a challenge encountered within the field of genomic medicine. The challenge relates to inconsistent understanding of the legality of sharing health (including genetic) data about one person to aid the interpretation of clinical significance of gene test results returned to another. As noted above, traditionally consent has only been implied to disclosure for purposes relating to an individual's *own* care. Disclosure of identifiable data to a clinician with no responsibility for an individual's care, in order to inform the care provided to another, falls outside that traditional understanding.

To assess the nature and scale of any challenge to bringing such disclosure within the scope of a valid consent one must understand the information requirements. Of course, that is not *all* that one would need to understand. One would also, for example, need to be clear on the requirements regarding the *voluntariness* of a consent, what might constitute valid *communication*, whether there are substantive constraints upon *permissible breadth*, etc. However, amongst these issues is the question of what information an individual would need to be provided with in order for any consent given to be valid. There is currently no clarity regarding the information provision requirements for a valid consent relevant to an action for breach of a duty of confidentiality.

Without clarity in relation to the information requirements, it is impossible to be sure when consent might avoid a breach of a duty of confidence or to be clear about the extent to which the requirements of a valid consent under the law of confidence are consistent with the requirements of a valid consent in other areas eg in data protection law (under the Data Protection Act 1998 or the soon to be in force General Data Protection Regulation). For those processing confidential patient data, and subject to the requirements of both the common law and data protection, this creates unnecessary and unfortunate uncertainty.

In this context, we should also recognise the contemporary significance of recommendations made by the NDG in relation to a national consent or opt-out model for data sharing in relation to identifiable health data. In her report, the NDG did not seek to adjust the underlying requirements of a valid consent but, instead, considered

6 We consider some of these cases below.

7 For discussion of the problems with such an assumption, see G Laurie, 'Liminality and the Limits of Law in Health Research Regulation: What are We Missing in the Spaces In-between' (2017) 25 Medical Law Review 47.

when an individual consent is required and *when* and *how* individuals should be able to opt-out of processing that has a legal basis other than consent. Given the current recommendation that a registered opt-out will *not* apply to data flowing with a patient's explicit consent, an understanding of the requirements of a valid consent is crucial to understanding the operation of the national opt-out model.[8]

There are a number of things that this article does not do. We do not consider the question of legal bases for disclosure other than patient consent. We set aside any question of a statutory or public interest justification for use or disclosure of confidential patient data. We do not consider the requirements of a valid consent under the law of confidence generally: voluntariness, communication, permissible breadth, etc. Also, for reasons of space, we do not here provide any extended consideration of the information provision requirements of a valid consent under data protection law. We focus only on the information requirements of a valid consent from the perspective of the common law duty of confidentiality. This is just one part, but an important part, of a picture that must be completed if, alongside separate consideration of these other things, we are to be clear on the legal requirements applicable to flows of confidential patient data and consistency of those requirements across the legal landscape.

As the way that healthcare is provided and the methods by which a healthcare system may learn become increasingly sophisticated, it is important to establish the preconditions for confidential data to flow. Practice must be able to confidently resist legal challenge. Relating to this, we need to debate the need for *alternatives* to consent as legal bases for data to flow in the future. However, without properly understanding the possibilities for data to flow because of consent, one cannot properly understand the need for any alternative to consent.

We demonstrate that, at least so far as the common law duty of confidentiality is concerned (and the associated tort of misuse of private information)—while any valid consent needs to be appropriately informed—the information required to achieve a valid consent should not be modelled on the informational levels the law requires to achieve 'informed consent' in the context of medical treatment. Instead, in the context of confidential data, comparison may be more appropriately made with legal approaches to consent, which are considered sufficient to establish valid consent even if that consent is *relatively uninformed*.

Our intention here is not to dilute the significance of respect for individual autonomy. Nor is it to undermine important efforts to improve the extent to which individuals are able to engage effectively with the ongoing process of consent or understand how data is used within the healthcare system.[9] On the contrary, we will suggest that a proper understanding of the information provision requirements of a valid consent from a legal perspective might lead to people being *more* involved in decisions about the use of confidential patient data into the future than might follow a more stringent understanding of relevant information requirements: this understanding of the requirements may undercut reliance upon alternative legal bases.

8 *National Data Guardian for Health and Care, Review of Data Security, Consent and Opt-outs* (June 2016).

9 J Kaye and others, 'Dynamic Consent: a Patient Interface for Twenty-First Century Research Networks' (2015) 23 European Journal of Human Genetics 141.

We also wish to avoid any suggestion that a valid consent is *sufficient* to ensure proper governance of health data. We support those who would argue that a valid consent is understood to be but one part of an effective regulatory landscape.[10] Our argument here is that, from a legal perspective, consent may defeat a claim of breach of confidence where use or disclosure is consistent with what a person may reasonably be understood to have agreed, even if his or her expectations regarding use or disclosure were only informed in a general sense.

The argument proceeds through three parts. In Part One, we focus on the informational requirements that have developed in the context of consent in the tortious context. A distinction is made in tort between the informational requirements of 'real' consent and 'informed' consent. In Part Two, we explain why, in the context of a consent to the disclosure of confidential patient data, the information levels underpinning a consent in the law of confidence are more closely aligned with those required for a 'real' consent than an 'informed' consent. This leads to Part Three, to a consideration of the practical implications: What information must be provided in order to gain a valid consent to the use of data in order to avoid a breach of confidentiality?

Without clarity regarding the necessary information levels, there is a genuine risk that the law will be understood to present hurdles to proceeding on the basis of a consent. If the minimum information provision requirements *can* be met, then there is one less reason to find an alternative legal basis. If the requirements of consent are overstated, then the consequence may be that individuals are denied the choice and control they might otherwise enjoy.

II. PART ONE: DISTINGUISHING BETWEEN 'REAL' CONSENT AND 'INFORMED' CONSENT

One reason there might have been little discussion of the requirements of a valid consent to the use of confidential data is that there is an assumption that there is nothing special about the legal requirements of a valid consent relating to the duty to maintain confidence.[11] However, this assumes that the requirements of a legally valid consent are consistent and clear. There is widespread agreement that to be legally valid, a consent must be freely given by someone with capacity, it must be underpinned by relevant information and communicated.[12] Although it is accepted that a consent needs to be underpinned by relevant information, the level of information adequate to achieve legally valid consent has varied over time and according to the function of consent in the circumstances.[13] English law has built up a detailed jurisprudence in the context of consent to medical intervention. However, even in this context, the

10 G Laurie and others, 'On Moving Targets and Magic Bullets: Can the UK Lead the Way with Responsible Data Linkage for Health Research?' (2015) 84 International Journal of Medical Informatics 933.

11 Thank you to Professor Roger Brownsword for making this point.

12 Mental Capacity Act 2005 s 3.

13 Alasdair Maclean distinguishes between legal and ethical consent asserting that 'there are two "consents"; one a legal consent required by the law of battery, the other an ethical consent predicated on the patient's right to autonomy, which must be obtained if the professional is to avoid liability in negligence'. A Maclean, *Autonomy, Informed Consent and Medical Law: A Relational Challenge* (Cambridge University Press 2009) 195. We would note that *both* consents respect a right to autonomy. They are, however, associated with different information requirements.

question of what information is needed to secure a valid consent to medical intervention depends on whether an individual is being asked to consent to physical intervention, or to running risks associated with that intervention. Furthermore, even where the law is clear that an 'informed consent' is required, the jurisprudence over the last 30 years has been unable to clearly articulate the standard used to judge whether a consent is properly 'informed' or not.[14] The purpose of this piece is not to argue that there is an entirely new set of specifications for a valid consent to the use of confidential patient data, indeed it is assumed that the standard requirements of capacity, voluntariness, adequate information, and effective communication, apply. Instead, this piece considers what amounts to adequate information such that a person's consent to use of her information would mean that such use would not amount to a breach of the common law duty of confidentiality. We look at the differing and sometimes unclear informational requirements of a valid consent to medical intervention and examine where the information provision requirements of a valid consent to the use and disclosure of confidential patient data might fit within this matrix.

In the context of medical interventions, the patient gives permission for two things: the running of personal risks that are associated with an intervention and the physical intervention itself.[15] The amount and type of information that patients will need in order to give permission varies between these different aspects of a medical intervention. In relation to a permission to run particular risks, a patient's permission expresses her right to choose in the light of relevant alternatives, which may have different risks.[16] There is no equivalent need to inform an individual of alternatives, or associated risks, in order to respect her right to choose whether to permit physical interference. The difference is reflected in the informational levels the law requires. Consent giving permission to physical interference involved in medical treatment is governed by the tort of battery, where the legal term of art 'real' consent[17] is used to depict the conditions required to achieve legal validity. In contrast, consent which gives permission to run personal physical risks is governed by the tort of negligence, where the more familiar term 'informed' is used to reflect the conditions for achieving legal validity.

14 In *Sidaway v Board of Governors of the Bethlem Royal Hospital and the Maudsley Hospital* [1985] UKHL 1 the duty to provide information was based on the professional standard set in *Bolam v Friern Hospital Management Committee* [1957] 1 WLR 582. However, some judicial unease at this approach was evident in *Pearce v United Bristol Healthcare NHS Trust* [1998] EWCA Civ 865 and even more so in *Birch v University College Hospitals NHS Trust* [2008] EWHC 2237 (QB) which led to dicta doubting this standard for setting informational requirements. This move away from the professional standard was confirmed in *Montgomery v Lanarkshire Health Board* [2015] UKSC 11. However, until more jurisprudence is established, it might be argued that how content is imported into this informational standard is not clear.

15 On this, see Maclean (n 13).

16 This would usually be a less risky procedure (see *Birch v University College Hospitals NHS Trust* [2008] EWHC 2237 (QB)), but *Montgomery v Lanarkshire Health Board* [2015] UKSC 11 suggests that patients should also be informed about riskier alternatives.

17 The term 'real' consent can be considered a legal term of art which reflects what is considered to be a valid consent in the particular context of consent to medical physical interference, such that the interference does not amount to a battery. We are grateful to Edward Dove for suggesting that we explain this.

A. The Tort of Battery and 'Real' Consent

If a clinician subjects a patient to physical interference, then without that patient's valid consent, and absent alternative legal justification, they commit the legal wrong of battery. To be able to consent to the physical intervention, the patient needs to know what that physical interference will entail. Most battery cases concerning medical treatment have involved situations where an intervention was performed against the patient's will,[18] where a different intervention to the one consented to was performed,[19] or where patients have been deliberately and fraudulently misled.[20] Thus the essence of most cases is not whether adequate information has been provided, but whether *any* relevant information has been provided. That said, although not typically an issue, the question of adequacy has been considered by the courts.

In *Chatterton v Gerson* the Court considered what information was required before a patient could give a valid consent to a medical physical interference which would prevent a subsequent action in battery. Bristow J said:

> . . . once the patient is informed in broad terms of the nature of the procedure that is intended, and gives her consent that consent is real[21]

Thus, the patient only needs to understand the general nature of the operation 'in broad terms' before the law considers this consent to be valid to permit the physical intervention and, therefore, terms it 'real'. Information about the general nature of a single medical procedure might not be particularly extensive or complicated. The minimal level of information required to achieve 'real' consent does not include a requirement to disclose information about the risks associated with the physical interference or any alternatives.[22]

For this reason, 'real' consent may be relatively easily achieved. It is notable that we have not seen legal challenge in England arguing that the information given about the nature of a medical treatment was insufficient to make the patient 'broadly aware'. It might be argued that the ease of gaining 'real' consent in this context is one of the things that has enabled consent to become a cornerstone of English medical law. Consent is readily achievable; so, professionals need not look for alternative legal bases to protect themselves or their patients.

B. The Tort of Negligence and 'Informed Consent'

If a clinician subjects a patient to non-negligent risks associated with an intervention without a valid consent to those risks, if one of these risks eventuates, then the non-disclosure could be actionable in negligence. It is clear that the information required for an 'informed' consent is different to the information required for 'real' consent. In giving an 'informed' consent you still need to be aware of the nature of the procedure

18 *Re B (Adult, refusal of medical treatment)* [2002] 2 All ER 449; *Re C (Adult, refusal of treatment)* [1994] 1 All ER 819.

19 *Devi v West Midlands RHA* [1980] CLY 687.

20 *Appleton v Garrett* (1997) 8 Med LR 75.

21 [1981] QB 432, 443.

22 For an in-depth discussion of the different requirements of 'real' consent and 'informed' consent, see Maclean (n 13).

to which you are consenting,[23] but this information is required as a basis for the information about risks which arise in the context of the intervention. The concept of 'informed' consent provides a mechanism for patients to consent to the risks of a procedure as opposed to consenting to the physical intrusion of the procedure in and of itself. Furthermore, it is when we begin to talk about consenting to risk, that the concept of alternatives becomes relevant. A person can only make an accurate assessment of the risk she is prepared to run, if she knows about the risks associated with alternatives and with non-intervention. It is this information that sits at the heart of *informing* an 'informed consent'. [24]

C. Why Not 'Inform' a 'Real' Consent?

A failure to disclose risks and benefits, or to compare the proposed physical intervention with alternative courses of action, will not render a 'real' consent invalid but it will mean that the patient cannot have consented to run the risks associated with the intervention and thus that consent cannot be said to be 'informed'. In *Chatterton v Gerson*, Bristow J felt that the action of battery was inappropriate in cases where the doctor had acted in good faith, and in the interests of the patient, but in doing so had been negligent in failing to disclose a risk inherent in the recommended treatment.[25] Battery is an intentional tort and has historically been associated with notions of bad faith.[26] Thus, it is perhaps not surprising that the courts find it inappropriate to hold that doctors who act in a patient's best interests, but inadvertently fail to disclose a risk, have battered the patient.

At this point, it is worth emphasising that in providing individuals with information about the *risks* associated with medical intervention we are not seeking to protect them from harm *per* se. We are seeking to ensure persons can make an autonomous choice whether to accept the risks associated with that intervention. This goes beyond recognising a right to choose on the part of the person giving consent; it recognises that the individual obtaining the consent has to have a responsibility to inform that choice. This is a responsibility not recognised in the tort of battery. Hence, a 'real' consent need not be 'informed'.

---

23 In principle, a claim that the wrong intervention was performed could be brought in negligence. Although in *Chatterton v Gerson* (n 21) 443 Bristow J felt that trespass would be the appropriate cause of action in this case.

24 It is clear in English law that doctors have a duty to inform patient of lower risk alternatives to the treatment that is posed (*Birch v University College Hospitals NHS Trust* [2008] EWHC 2237 (QB)). However, it might be argued that *Montgomery v Lanarkshire Health Board* [2015] UKSC 11 imposes a duty to inform patients about other possible procedures irrespective of whether they have a lower risk. In *Montgomery*, the risk issue was complicated by the fact that the non-disclosure of information concerned the risk of shoulder dystocia in child birth. Child birth involves risk to both mother and child. In that case the Supreme Court held that the doctors had a duty to inform the mother about the alternative of caesarean section which had a higher risk of morbidity and mortality for the mother than the natural birth.

25 *Chatterton v Gerson* (n 21) 442, Bristow J relying on the judgment of the Ontario Court of Appeal in *Reibl v Hughes* (1978) 21 OR (2d) 14.

26 *Wilson v Pringle* [1987] QB 237.

D. Setting Standards in the Information Requirements of 'Informed' Consent and 'Real' Consent: Whose Perspective Counts?

In the context of consent to medical treatment, English law provides content to the information requirements by reference to the perspectives of the parties to the consent. Here again we see a distinction in the approach taken for 'real' consent in battery and 'informed' consent in negligence.

In relation to 'real' consent, there is little judicial discussion about how standards are set regarding the relevant information content. However, in *Chatterton v Gerson* Bristow J. says:

> the duty of a doctor is to explain to the patient what he intended to do and the implications of that action in a way that a careful and responsible doctor would do in similar circumstances.[27]

This suggests that the standard for determining what information should be disclosed to make a patient 'broadly aware' of the nature of the medical treatment, thereby obtaining 'real' consent and avoiding an action in battery, falls to be determined by the medical profession.

Although medicine, especially in the context of information disclosure, is not an exact science, the medical profession has the opportunity to articulate a relatively unified professional view about what is considered to be relevant information about a particular procedure. Thus, setting informational level standards by reference to the profession can provide some consistency and certainty for those seeking consent. If the level of information required to avoid a battery on the basis that there is a 'real' consent requires patients to be made 'broadly aware' of the nature and purpose of the action by reference to the reasonable doctor's view of what is relevant, then gaining consent need not be particularly onerous or complicated.

The English courts originally took a similar position to setting standards in informational levels in 'informed' consent. In *Sidaway v Board of Governors of the Bethlem Royal Hospital and the Maudsley Hospital*,[28] relying on the *Bolam* test,[29] the House of Lords held that for the patient to be adequately informed, the risks which need to be disclosed should be determined by what the medical profession thought it reasonable to disclose. However, in *Montgomery v Lanarkshire Health Board* the Supreme Court was invited to depart from *Sidaway* and reconsider how standards are set in this context. The Supreme Court considered that the doctor's duty to disclose information about risks and alternative treatments should no longer be based on *Bolam.* Instead the court held that the doctor is:

> under a duty to take reasonable care to ensure that the patient is aware of any material risks involved in any recommended treatment, and of any reasonable alternative or variant treatments. The test of materiality is whether, in the circumstances of the particular case, a reasonable person in the patient's position would

27 *Chatterton v Gerson* (n 21) 432.

28 [1985] UKHL 1.

29 *Bolam v Friern Hospital Management Committee* [1957] 1 WLR 582.

> be likely to attach significance to the risk, or the doctor is or should reasonably be aware that the particular patient would be likely to attach significance to it.[30]

Thus, in the context of medical treatment, the level of information that a patient requires before they can give an 'informed' consent is referenced to the patient's perspective, and not the professionals'.

E. A Distinction With or Without a Difference?

At first sight we might question whether there are significant differences between the views of professionals and patients regarding relevant information in the context of medical treatment. However, the number of legal challenges concerning non-disclosure of medical risk information suggests that patients do often want more information than professionals think they need to disclose.[31] The GMC has noted this discrepancy between the views of professionals and patients in the context of the use of healthcare data:

> Professionals are, of course, people so, at one level, they should appreciate the needs and concerns of members of the public. However, they also have their own professional interests and may become inured to concerns that might impact upon them as citizens, especially as they are often coping with more immediate and pressing issues when dealing with patients, so may not reflect the values and opinions of the average member of the public.[32]

Support for the argument that practitioners' views differ from the views of people using services can also be found generally in relation to the issue of running risks,[33] which we know is at the heart of 'informed' consent.

In the light of differing professional and public attitudes to information about risks, *Montgomery* recognised that an approach to setting informational levels based on medical professional standards might not provide the information that patients feel they need. One consequence of this is that there is arguably now significantly less clarity concerning what information needs to be disclosed in the context of 'informed' consent as compared to 'real' consent. Unlike procedural information about the nature of the treatment, information about possible risks and alternatives can be extensive, complicated, and sometimes conflicting. Furthermore, patient perspectives about the relevance of specific risk information are likely to be diverse. Following *Montgomery,* the profession cannot come together collectively to put boundaries

30 [2015] UKSC 11, Lord Kerr and Lord Reed 87.

31 A few high profile ones are: *Sidaway v Board of Governors of the Bethlem Royal Hospital and the Maudsley Hospital* [1985] UKHL 1; *Montgomery v Lanarkshire Health Board* [2015] UKSC 11; *Chester v Afshar* [2004] UKHL 41; *Al Hamwi v Johnston and another* [2005] EWHC 206 (QB) and *Pearce v United Bristol Healthcare NHS Trust* [1998] EWCA Civ 865.

32 General Medical Council, *Public and professional attitudes to the privacy of healthcare data; a survey of the literature,* 30 August 2007.

33 S Carr, *Enabling Risk, Ensuring Safety: Self-directed Support and Personal Budgets* (Report 36, Social Care Institute for Excellence 2010).

around the information that is required based on professional perspectives. If this results in fresh uncertainty and prompts, as a defensive response, increasingly lengthy and complex consent forms, then—paradoxically—genuinely informed consent may be made harder to achieve. This is a point that has been explored by others and on which we need not linger.[34] As this discussion demonstrates, the information disclosure burden in the context of consent to medical treatment is heavily focused on 'informed consent' to personal risk, rather than 'real' consent to physical intervention.[35] This is because the information concerning the single medical intervention is often clear and concise. The clinician may only need to disclose a small amount of information to avoid an action in battery. The nature and amount of the potentially relevant risk information means that it is much more difficult to be clear about what needs to be disclosed and that often there will be a higher informational burden attached to an 'informed' consent.

III. PART TWO: CONSENT TO THE USE OF HEALTH DATA

We have outlined the information requirements associated with a valid consent from the perspective of both the tort of battery and the tort of negligence. We have seen that they vary in both the extent of the information that must be provided in order for a consent to be adequately 'informed' or 'real' and also the perspective from which one must assess adequacy. Against that backdrop, we will now consider the informational requirements of a valid consent from the perspective of the common law duty of confidentiality.

At the outset we might draw parallels between the tort of battery and the common law duty of confidentiality. Both are grounded in the public interest and the equitable notion of good faith. Both incorporate an element of wrongdoing. Battery is an intentional tort and breach of confidence suggests some unauthorised or unjust use or disclosure of confidential data. The courts have recognised it to be in the public interest to protect people from a *misuse* of confidential data—indeed, we now talk about a tort of misuse of private information as well as a breach of a duty of confidence.[36] Private data is now recognised to be worth protecting as an aspect of human autonomy and dignity.[37] In order to protect people from privacy interferences there is a need to ensure people have a measure of control over the use of confidential data, including its onward disclosure. If an individual gives consent to the use of confidential data, then it is the intended use and disclosure to which she must agree. An individual's privacy, autonomy, and dignity are protected through her authorisation of use.

In these terms, protection from misuse does not require the party receiving confidential data to provide information about any risks associated with disclosure: it requires only that confidential data is used consistent with authorisation and an

34 Manson and O'Neill have previously examined the limits of 'informed' consent based on impossible procedures and standards. See N Manson and O O'Neill, *Rethinking Informed Consent in Bioethics* (Cambridge University Press 2007).

35 The cases concerning inadequate information disclosure in the context of medical interventions are negligence cases concerning non-disclosure of risk, rather than battery cases concerning failure to disclose all the information required to make the patient 'broadly aware' of the nature of the medical treatment.

36 *OBG Ltd and another v Allan and others* [2007] UKHL 21, [2008] 1 AC 1 [255].

37 *Campbell v MGN Limited* [2004] UKHL 22 (Lord Hoffmann) [50].

individual's reasonable expectations of privacy.[38] Importantly, a risk of *misuse* is not a risk to which one could usually consent in any case. To explain this point, we must make a distinction between negligent and non-negligent risks. In 'informed' consent the risks which are disclosed are risks of things that might happen *without any negligent or criminal action*. Information is not provided about risks of negligent or unlawful activity because there is no evidence that people can consent to negligence in the context of medical treatment, or moreover, that professionals can rely on consent to avoid their duty not to treat a patient negligently.[39] However, the risks that concern people with regard to the use of data for medical purposes[40] are typically associated with negligent,[41] unlawful[42] or unauthorised use: data being lost, hacked, provided to third parties, and/or used for purposes other than those described at the time that consent is given.[43] The disclosure of the risks that negligent or unlawful things might happen would not provide the individual or organisation with a legal flak-jacket:[44] they could not rely on consent to argue that they are not responsible for a breach of confidence which occurred through their negligent, unauthorised, or illegal activity.

As an aside, we note that there is a defence of *volenti* to the tort of negligence, based on the premise that a person's claim for injury can be defeated if they can be said to have voluntarily assumed the risk of injury where that injury is caused by negligence. However, even though in some cases the courts have treated knowledge as synonymous with consent,[45] knowledge of, or willingness to take a risk, are not generally seen by the courts as the same as consent.[46] Moreover, it is well established that the defence of *volenti* only goes so far.[47] It is difficult to establish,[48] applying only in situations where there is a very high risk and the claimant has done something reckless implying moral culpability.[49] There is no evidence in English jurisprudence that the

38 The concept of 'reasonable expectations' is more fully discussed later.

39 The defence of *volenti* has had no application in this context. See discussion below.

40 The purposes for which health data may be used are many and varied. For the purposes of this article we restrict ourselves to a consideration of medical purposes as defined by s 251 NHS Act 2006 and/or within para (h), sch 3, DPA 1998.

41 The 2015 Mid-Year Cyber Risk Report found that for healthcare specifically, most data breaches are a result of employee negligence. *Surfwatch Labs Situational Awareness Report: 2015 Mid-Year Cyber Risk Report: Risk Intelligence Trends and Cybercriminal Avenues of Approach*; E Snell 25 August 2015 Negligence Top Health Data Breach Issue, Report Says <http://healthitsecurity.com/news/employee-negligence-top-health-data-breach-issue-report-says> accessed 26 February 2016; *National Data Guardian for Health and Care* (n 8) 2.42–2.43.

42 See the recent criminal cyber-attack which affected the NHS: <https://www.theguardian.com/society/2017/may/12/hospitals-across-england-hit-by-large-scale-cyber-attack> accessed 27 June 2017.

43 Harms are typically associated with *abuses* of data. For categorisation of such abuses, and description of associated harms, see G Laurie and others, *A Review of Evidence Relating to Harm Resulting from Uses of Health and Biomedical Data* (Report for Nuffield Council of Bioethics Working Party on Biological and Health Data, 2014).

44 Lord Donaldson referred to consent acting as a legal flak jacket protecting the doctor from litigation in the context of minors (and parental) consent to medical treatment in *Re W (a minor) (medical treatment)* [1992] 4 All ER 627 at 635.

45 *Morris v Murray* [1990] 3 All ER 801.

46 *Dann v Hamilton* [1939] 1 KB 509 and *Nettleship v Weston* [1971] 2 QB 691.

47 Evidence of this is particularly clear in the context of sport. See, for example, *Condon v Basi* [1985].

48 See, for example, *Smith v Baker* [1891] AC 325; *Dann v Hamilton* [1939] 1 KB 509; *Baker v T E Hopkins & Son Ltd* [1959] 1 WLR 966 and *Condon v Basi* [1985] 2 All ER 45.

49 See, for example, *Morris v Murray* [1990] 3 All ER 801.

defence of *volenti* is applicable to absolve a medical practitioner of negligence where they inform their patient of a risk that they will be negligent in a medical intervention.

Thus, the notion of negligent, unlawful, or otherwise unauthorised data breach or risk thereof, is unlikely to form the essence of a consent to the use of health data. Nevertheless, this does not mean that it would not be good professional practice to draw the person's attention to the fact that there are general risks of negligent, illegal, or unintended activity. However, the purpose of disclosure of this information could not be to allow the person to consent to the running of that risk. Thus, it should not be understood to be a requirement of a valid consent.

To illustrate the point, consider this example. Imagine an individual gives consent to the use of her data in a medical research project. Informing her that a renegade research assistant might publish her confidential data on a social media platform without permission, would not protect the research assistant from an action for breach of confidence. Knowing the possibility of such a risk *might* inform her decision to participate—it is possible that it may even be a risk she would want to be aware of—but it is not a risk to which she can consent. Indeed, to impose such a responsibility to provide information in respect of negligent, unlawful, or otherwise unauthorised use would *exceed* the responsibilities associated with even an 'informed consent' to medical treatment.

Returning to the distinction drawn between negligent and non-negligent risks, we turn now to consider the relevance of '*non-negligent*' risks to our argument. Even though most of the risks likely to be of concern relate to abuses: negligent, unauthorised, or illegal activity, it is possible to envisage a situation where a risk, perhaps of identification, might arise without wrongdoing on behalf of those who are under a duty of confidence to the data subject. Imagine the situation where a researcher obtains identifiable health data from a person and uses this in a research project. The researcher gained consent to the use of this identifiable data and consent to the publication of this data in anonymised form. However, through no fault of the research team, the person is subsequently identified when the published anonymous research data is combined with other data which becomes legitimately publically available. In this context, there does not appear to be a breach of confidence. As argued earlier, as with the tort of battery, breach of confidence requires wrongdoing. Those under a duty to maintain confidence have not misused the information and have not acted unjustly. Let us imagine they have done everything that could reasonably have been expected of them to protect confidentiality.

Nevertheless, one might argue that there is a wrong done: it was wrong not to tell the research participant of the possibility of (re)identification from the published data. However, *if* the non-disclosure of a non-negligent risk was a legal wrong, then it would be due to *negligent* non-disclosure of risk, not due to the publication of the anonymised data. Liability would be assessed under the law of negligence, not the duty of confidence. This is an important distinction. Not least of all because a failure to provide the information about risk would not invalidate the consent to the use and disclosure of confidential data *within* the scope of the authorisation. Here we begin to see a distinction between the law of confidence and the law of negligence parallel to the one we see between the law of battery and the law of negligence in the context of consent to medical treatment.

We should emphasise that there is currently no case law suggesting that a person gaining consent to use of patient data would be liable in negligence for non-disclosure of non-negligent risks, such as the risk that the data subject might subsequently be identified through no fault of the person gaining consent. We are considering only the legal circumstances under which information about non-negligent risks might have to be provided; that is, where a failure to provide the information was itself *negligent*. However, were the courts to decide that non-disclosure of the risk of non-negligent re-identification when gaining consent to the use of patient data is culpable in negligence, then we would point out that it does not follow that the high level of information and the requirement to assess materiality in the context of the particular case would follow necessarily as it applies in the context of consent to medical treatment. Further consideration of this point requires a paper on negligence rather than one on breach of confidence. However, given the arguments around a persistent non-negligent risk of re-identification of published anonymised data,[50] it may be sensible to always succinctly disclose this risk. This would be irrespective of the statistical level of the risk and without assessing materiality in individual cases. As we note above, disclosure of such risks may be good practice. They are not, however, required in order to avoid a breach of confidence.

If 'informed' consent focuses on consent to running risks, then there is no clear reason why the doctrine of 'informed' consent, and the need to set standards by reference to the patient's perspective, should set the informational focus in consent to the use of one's health data. Indeed, it seems that the kind of information that would be useful to patients who are being asked to give permission to the use of their health data is much more akin to the information required for a 'real' consent. That is, the information that concerns the nature and purpose of the use and disclosure intended. It is this that people are being asked to legitimise as opposed to potential negligent or unlawful activity.

However, even if what is required in the context of a consent to use of health data is a 'real' consent, we still may not get the same level of clarity and brevity regarding adequate information in the context of a consent to use of health data as is regularly achieved in the context of a single medical intervention. First, information about uses of health data is often varied and uncertain. Explaining a number of definite, probable, and possible uses by varying definite, probable, and possible entities, in a way which could be said to achieve a 'broad awareness' of what will happen, will include significantly greater information than that required to achieve 'broad awareness' in the context of a single medical intervention. Secondly, it does not follow that just because the professional perspective is privileged in the context of a real consent to physical interference, it will be similarly privileged in the context of a 'real' consent to confidential data use. However, removing the terminology of 'informed' consent and replacing it with the application of a clear legal principle of 'real' consent, coupled with an established standard for setting relevant information levels needed to achieve the 'broad

50 <http://www.independent.co.uk/life-style/health-and-families/health-news/anonymous-nhs-database-could-still-allow-patients-to-be-identified-expert-warns-10001783.html> accessed 11 May 2017. P Ohm 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymisation' (2010) 57 (6) UCLA Law Review1701.

awareness' required by 'real' consent, will provide greater clarity concerning the kind of information that *is* required to support a valid consent to the use of health data than we have now.

IV. PART THREE: SETTING STANDARDS IN BREACH OF CONFIDENCE AND MISUSE OF PRIVATE INFORMATION

Although there is little consideration of the informational levels which should underpin a valid consent in the context of the use of confidential data, the English courts have established a rich jurisprudence regarding how legal standards are set in the context of use of information which is confidential or private *without consent*. This may influence how content is determined in informational standards of consent to the use of confidential data.

In *AG v Guardian Newspapers* (No 2) Lord Goff defined the duty of confidence in broad terms:

> a duty of confidence arises when confidential information comes to the knowledge of a person (the confidant) in circumstances where he has notice, or is held to have agreed, that the information is confidential, with the effect that it would be just in all the circumstances that he should be precluded from disclosing the information to others.[51]

Protection equivalent to that originally offered by Lord Goff's broad principle is now found in the concept of 'reasonable expectation'. Thus, a duty will exist whenever a person knows or ought to know that another can reasonably expect his or her privacy to be protected[52] or, as Baroness Hale put it in *Campbell v Mirror Group Newspapers*:

> [W]hen the person publishing the information knows or ought to know that there is a reasonable expectation that the information in question will be kept confidential.[53]

According to Lord Hope, 'reasonable expectation' is determined by reference to 'a person of ordinary sensibilities' in the position of the person to whom the information relates.[54] Thus the circumstances will determine if a disclosure is consistent with an individual's 'reasonable expectations': only if a person of ordinary sensibilities could be said to have a 'reasonable expectation' that his or her data will not be disclosed, or not disclosed without authorisation, will such disclosure constitute an infringement of

51 [1990] 1 AC 109, 281.

52 *Campbell v Mirror Group Newspapers* [2004] UKHL 22 Lord Nicholls of Birkenhead 21, Lord Hope of Craighead 84 and Baroness Hale 137. In *Campbell*, the common law duty of confidence was interpreted so as to give effect to Art 8 of the European Convention on Human Rights, holding that the common law can address the misuse of private information. In the context of the facts in *Campbell*, Lord Nicholls felt that the more natural description was that the information was private and the essence of the tort was better encapsulated as misuse of private information. Sometimes information may be described as private and confidential and could qualify for protection by either tort. In other situations, information may be private but not confidential.

53 [2004] UKHL 22 Baroness Hale 134.

54 ibid (Lord Hope), 99. See also *Murray v Express Newspapers* [2008] EWCA Civ 446, 35– 36.

privacy and give rise to a cause of action for either breach of confidence or misuse of private information.

In *Campbell* Lord Hope said:

> Where the person is suffering from a condition that is in need of treatment one has to try, in order to assess whether the disclosure would be objectionable, to put oneself into the shoes of a reasonable person who is in need of that treatment.[55]

There is ambiguity here regarding whether standards of what would be objectionable in terms of disclosure of confidential data are referenced to the confider or the confidant. However, reading Baroness Hale and Lord Hope's quotes from *Campbell* together they seem to suggest that the standard is set by the professional who has a duty to consider the reasonable person's view. Once this consideration can be demonstrated, the professional has reached the required standard. However, in the particular context of the confidence of health data the courts had previously stated that it is the professional perspective and not the patient perspective which provides the content for the standard of care.

In *R v Department of Health Ex P Source Informatics*[56] Source Informatics was a database company that collected data on GP prescribing from prescriptions submitted to pharmacies and sold the information, without patient identifiers, to pharmaceutical companies for marketing purposes. The Department of Health issued a policy statement declaring that this was a breach of confidence because there was no consent to this use. Source Informatics sought judicial review of this policy statement. In the Court of Appeal, Simon-Brown LJ felt that the question for the court was whether the confider's privacy had been invaded by a breach of confidence by the pharmacists.[57] In his view:

> The confidant was placed under a duty of good faith to the confider and the touchstone by which to judge the scope of this duty and whether or not it has been fulfilled or breached is his own conscience, no more and no less.[58]

Thus, the question in *Source Informatics* was: would a reasonable *pharmacist's* conscience be troubled by the proposed use to be made of patients' prescriptions?[59] It was common for pharmacies to be paid for access to their anonymised prescription data,[60] demonstrating that pharmacists were generally not troubled by this use. In the event, the court found the patient's privacy interests were not engaged. According to Simon-Brown LJ the patient's only legitimate interest was in the protection of his privacy and this was safeguarded by anonymization.[61]

---

55 ibid (Lord Hope), 98.
56 [2000] 1 All ER 786.
57 ibid (Simon-Brown LJ), 797.
58 ibid (Simon-Brown LJ), 796.
59 ibid.
60 ibid (Simon-Brown LJ), 788.
61 ibid (Simon-Brown LJ), 797.

It seems most likely that the approach taken in *Source Informatics* is now best understood to have been overtaken by the approach taken in the more recent *Campbell* case. The courts will require a professional acting in good conscience to try to 'put oneself into the shoes of a reasonable person' in the position of the confider. That is, for the professional viewpoint to be expected to take account of public and patient attitudes. There is consistent and clear empirical evidence to suggest that the use of patient data for particular purposes, eg commercial purposes, *is* troubling to patients and the public (discussed further below). Thus, patients would likely have been troubled by the commercial marketing use of data in *Source Informatics*, they just did not know about it.[62] *Source* is not the only example of professionals sanctioning the use of patient health data for commercial uses that patients are likely to find objectionable. The review of data releases by the NHS Information Centre (IC)[63] found that the IC had made four Data Sharing Agreements with three re-insurance companies despite the fact that it was clear that people object to their data being used by insurers.[64] This does not mean that patient and professional views about legitimate uses of patient health data *always* conflict. However, where there are conflicts, they could have a significant impact on the public perception of the ability of professionals or professional organisations to act as a guardian of confidential patient data. Any erosion of public trust may impede the ability to use patient data to its full potential.[65] Thus a move to recognise that a professional's viewpoint must be informed appropriately by the 'reasonable expectations' of those whose information they handle is to be welcomed.

In the context of the uses of health data which might be complex and varied,[66] the professional obtaining consent is arguably in a better position than the patient to determine what information will make the patient 'broadly aware' of what will happen to their data. However, in the context of the common law duty of confidentiality, a move by the courts away from the professional conscience perspective reflected in *Source* to one that recognises the relevant standard to be what a professional ought to understand to be the 'reasonable expectation' of a patient in the circumstances may do more to engender public trust. There is the potential to allow professionals to collectively determine what is reasonable, *but* also to insist that in doing so, the significant evidence of public and patient attitudes[67] is taken into account. This leads us to the

62 Further because their privacy interests were not engaged, in that they could not be identified because the information was effectively anonymised, they did not qualify for protection of their interest in their data only being used in projects which they did not object to. Precluding disclosure of information to others to protect the confider's private information *per se* is the classic interpretation of the interest in confidence or privacy. However, as the disclosure and use of heath data for multiple and diverse propose grows, the duty of confidentially has evolved to protect the confider against uses of their data that they do not find agreeable, rather than an objection to people knowing information about them *per se*.

63 Review of Data Releases by the NHS Information Centre Sir Nick Partridge 17 June 2014, para 27.

64 Indeed, this objection was acknowledged in the report, ibid.

65 We know from Care.data that lack of public trust can have a significant impact on the ability to use health data. See the All Party Parliamentary Group for Patient Involvement in Health and Social Care. Care.data Inquiry, November 2014.

66 Which precludes the achievement of 'informed' consent in Manson and O'Neill (n 34).

67 Wellcome Trust, *Summary Report of Qualitative Research into Public Attitudes to Personal Data and Linking Personal Data* (2013); *Royal Statistical Society Response to the Department of Health on Protecting Health and Care Information in England: A Consultation on Proposals to Introduce New Regulations* (August 2014); Wellcome Trust, *The One-Way Mirror: Public Attitudes to Commercial Access to Health Data* (March 2016).

question what information needs to be provided in practice to generate a 'reasonable expectation' of a use such that a person can be said to be 'broadly aware' of it?

A. Generating 'Reasonable Expectations' in 'Real' Consent: What Information is Needed?

In the context of use or disclosure of a person's health data, 'reasonable expectations' of privacy will encompass expectations about when confidential data may or may not be shared. At the outset we noted that health professionals do not generally ask patients whether they can share their health data with other members of the health care team. The basis of that sharing is, nevertheless, understood to be the patient's consent. There is a professional assumption that patients reasonably expect sharing necessary to provide safe and effective care when the patient consents to receive that care.[68] Guidance recommends that information is 'readily available'[69] about such sharing[70] but there is no suggestion that, if a specific disclosure has not been brought to the attention of the patient, then a lack of information provision will render consent invalid. How far does the information which should be 'readily available',[71] but not necessarily specifically brought to a patient's attention, extend? What lengths must a professional go to provide specific information prior to a consent to use of confidential data?

There are likely to be very different levels of understanding of the regular uses of confidential patient data, particularly as they extend beyond an individual's care. Uses of confidential patient data for purposes beyond individual care, could be multiple and varied: including but not limited to the management of health and social care services (including commissioning of services), service evaluation and auditing quality of care, public health purposes (including health protection and health improvement), education and training, as well as health research and use by commercial entities. Each of these uses may involve disclosure to different organisations and persons. There are so many varied and diverse uses to which that information might be put that if being 'broadly aware' *does* require the patient be aware of more than the simple fact that their health data will be further used or disclosed, then even a 'real' consent may require information be provided specifically about a significant range of uses.

Although there is general support for the use of health data to provide public health benefits,[72] there are nuances within that support, and different uses of patient health data by different organisations enjoy different levels of acceptance.[73] For example, work done by Wellcome has found that it is more acceptable to disclose health data to universities and charities than to commercial organisations. Further acceptability declined sharply where the intended disclosee was a private provider either inside or outside the heath sector.[74] People did show some support for specialist analytics and research companies working closely with the NHS participants, pharmaceutical companies, and retail and pharmacy sectors having their data, but this was only if the

68 *Confidentiality: Good Practice in Handling Patient Information* (January 2017).
69 ibid, para 28 b.
70 ibid paras 10 and 28 b.
71 ibid.
72 See n 67.
73 Wellcome Trust, *The One-Way Mirror* (n 67) .
74 ibid 9.

purpose demonstrated some public benefit. On the other hand, most people found it unacceptable for insurance companies and marketing companies to have their data because they could not perceive a public benefit. They also erred on the side of caution and opposed sharing with a commercial organisation where the purpose was uncertain.[75] This work shows where information disclosure requirements should focus in order to adequately inform a 'real' consent: it is in relation to these uses that people do not generally either expect or accept as appropriate that there is a need to give more granular information. This is not to suggest that *no* information would need to be given to underpin a consent to a use that is generally acceptable in order for people to expect it. Indeed, there may be a difference between what people find acceptable and what people reasonably expect.[76] The argument is that evidence that a use is unacceptable to many is evidence that more effort should be made to ensure that people are aware if it is an intended use: without that effort it will be more challenging to describe it a 'reasonable expectation' that such use will follow consent. So, for example, specific information should be given about any uses that might not benefit the patient community.[77] In this way, evidence of public opinion on acceptability of use is a first step to determining how granular the need for information to establish a reasonable expectation that the use will follow consent should be.

The need for specific information to be given prior to a valid consent could be minimised by promoting a general awareness of the uses of patient data. If a particular use is recognised to be common knowledge and thus obvious to a person as a consequence of consent, then only minimal information could be provided about that use during the consent process itself without undermining the validity of that consent. However, it is unlikely that raising public awareness would generate a 'reasonable expectation' of use in the context of a use which evidence shows the public generally find unacceptable, such that minimal information about that use could then be given in the process of gaining consent. In the case of uses which the evidence suggests the public finds contentious, much greater weight would be put on giving the individual detailed information about the particular use in the act of gaining their consent before they could be said to 'reasonably expect' the use to be authorised by their consent.

The position that we are advocating is one that allows consent to be the basis of disclosure and use of health data; the responsibilities regarding information provision are not disproportionate, but they should ensure that the consent is 'real' and that people are informed about those things that are most likely to be considered material. Professionals do not, however, have to subjectively assess materiality in every case: there is scope for professional guidance on what information needs to be provided to patients. Such guidance should take account of the evidence available on patient and public attitudes. The growing evidence concerning people's views on the acceptability of the use of their health data could be an important indicator of where specific information ought to be provided. Where the conditions of who can use the data and why

75 ibid 11.

76 Mark J Taylor and Natasha Taylor 'Health Research Access to Personal Confidential Data in England and Wales: Assessing Any Gap in Public Attitude between Preferable and Acceptable Models of Consent' (2014) 10 (15) Life Sciences, Society and Policy 1.

77 This was not the approach to information provision that the Health and Social Care Information Centre adopted when seeking to establish an opt-out consent system to Care.data.

are deliberately constructed to conform with those more likely to be readily accepted—being less likely to be surprising or contentious—then consent may be 'real' even on the basis of little fine-grained information. However, where data is to be used by organisations, or for purposes, that are less widely expected or supported (eg shared outside the NHS or the medical research context), then it will be important to provide significantly more information about these uses, and in more detail, before persons feel that they are 'broadly aware' of the nature of the potential uses such that they can be considered to have accepted them. The evidence gathered on attitudes to use of health data demonstrates where the focus should be if providing information about uses of health data is to be standardised by reference to public attitudes regarding the general acceptability of potential uses.

If our argument to accept as legally valid a relatively uninformed consent seems radical, then we would note that the courts *have* found that minimal information about a possible intended use can be sufficient to give the patient a 'reasonable expectation' that their information will be used in a particular way. In *R (on the application of W, X, Y and Z)* v *Secretary of State for Health*[78] limited patient data was passed by NHS Trusts to the Secretary of State for Health and then to the Home Office for the purposes of imposing immigration sanctions applicable in case of certain debts being owed to the NHS. The specified limited information contained name and date of birth of the patient and, where available, his or her address, nationality and travel document number with expiry date and details about the amount and date of the debt, and the NHS trust to which it was owed.

At first instance, the judge decided that due to the lack of clinical information it contained, the information did not reach the threshold of private or confidential.[79] The Court of Appeal rejected this and supported the position taken by professional guidance that all identifiable patient data held by a doctor or a hospital must be treated as confidential. The Court's position was informed by the fact that this approach *is* taken in *publicly available* professional guidance, which itself can be understood to reflect and inform the expectations of patients. However, despite establishing the general position, the Court of Appeal found that in the particular circumstances of this case, the information disclosed was not confidential or private vis-à-vis the Secretary of State or the Home Office:

> We do not see how overseas visitors who, before they are treated in an NHS hospital, are made aware of the fact that, if they incur charges in excess of £1,000 and do not pay them within 3 months, the Information may be passed to the Secretary of State for onward transmission to the Home Office for the stated immigration purpose can have any, still less any *reasonable,* expectation that the information will not be transmitted in precisely that way. They will, however, have a reasonable expectation of privacy in relation to the information vis-à- vis anyone else.[80]

78 [2015] EWCA Civ 1034.

79 [2014] EWHC 1532 (Admin) 45.

80 [2015] EWCA Civ 1034, 44 (emphasis in original).

Thus, as patients were made aware of the fact that treatment incurred charges, they were deemed to 'reasonably expect' and *to have accepted*[81] that their data would be shared with regard to those charges if the debt was not paid.

In *W, X, Y, and Z*, the purpose was not directly related to healthcare, nor was the organisation a health care provider. However, the Court was satisfied here because information had been provided, and had in the Court's view been accepted, in relation to the specific disclosure. Thus, the provision of some limited information created a 'reasonable expectation' regarding further use by a non-healthcare institution for non-healthcare purposes.

V. CONCLUSION

We have argued that basing the information needed to achieve a valid consent to the use of health data on the approach to obtaining 'real' consent in battery, could produce a workable consent model in the health data context. The minimal level of information required for a consent which avoids a battery in medical intervention could be sufficient to avoid breaching confidence in the context of use of patient health data. Nevertheless, even satisfying this requirement could require considerable amounts of information to be made available to patients if they are to be 'broadly aware' of all uses of their information which go beyond direct care. Hence, we have argued that a workable 'real' consent model can be constructed by ensuring that the level and granularity of the information which achieves 'broad awareness' reflects the growing evidence of people's concerns and, for that matter, their lack of concerns regarding the use of their health information. The law might achieve this granularity by referencing the information needed to achieve 'broad awareness' to the notion of 'reasonable expectations'. On this perspective, the information underpinning consent can focus on those uses which are likely to be unexpected or contentious. Targeting the granular information required to underpin consent to uses which would not be 'reasonably expected', alongside constructing the kinds of things that people's health data might be used for so that reasonable people are unlikely to find them contentious, will make consent achievable. This approach would do significantly more to protect patient autonomy than an approach to using confidential data that is not based on consent.

Insistence on requirements of an 'informed' consent that are ill-fitting to the majority of risks associated with the use of health data and are impractical in requiring individual assessments of materiality will drive reliance on alternatives to consent. We have argued that the informational standards in a consent to use of health data need not be understood to be so onerous as to be impracticable. If we are to maintain consent in the context of the use of health data, then the information requirements need

81 The importance of acceptance is illustrated by the counter-examples given: 'There may, however, be special circumstances where the position will be different. For example, the patient may have been admitted unconscious to the A&E Department of a hospital (for which no charges are made) and may have been transferred, still unconscious, to a hospital ward (where treatment does attract charges). There may also be emergency cases where the clinical staff cannot refuse treatment and where, in practice, the patient has no choice but to accept the terms on which it is offered. Furthermore, in some cases the patient may be vulnerable and/or unable to speak English'. [2015] EWCA Civ 1034, 45.

to be simple and workable to prevent the erosion of choice which follows unworkable informational requirements.

ACKNOWLEDGMENT

We are grateful to Professor Roger Brownsword and Edward Dove for reading and commenting on earlier drafts of this work.