JOURNAL OF MEDICAL LAW AND ETHICS; VOL. 3, NR. 1-2, 109-133, PARIS LEGAL PUBLISHERS © 2015

ARTICLE

From *X v Y* to care.data and beyond: Health Care Confidentiality and Privacy in the C21st: a Critical Turning Point?

Jean McHale*

Professor of Health Care Law University of Birmingham, Birmingham

Introduction

The confidentiality of patient information has long been seen as something critical to health care practice. From the days of the Hippocratic Oath doctors have been exhorted to keep their patients' secrets and this is also enshrined in health care professional ethical codes today.[1] Patient confidentiality can be seen as having a number of dimensions. It can be seen in terms of 'professional' confidentiality – an obligation placed upon the physician to maintain the confidentiality of personal information. It can also be seen as having a practical importance justified by reference to utilitarian analysis – without safeguards provided in relation to the confidentiality of patient information, individuals would in some instances be deterred from seeking treatment.[2] This may be particularly the case where disclosure of such patient information may have adverse consequences for the individual in terms of stigma and discrimination. A notable illustration of this arose in relation to HIV and AIDS when in the early years of the identification of the disease in the USA there was evidence that individuals were being deterred from seeking treatment due to the adverse impact of such a diagnosis,[3] and the question of stigma and

* DOI 10.7590/221354015X14319325750197

1 See e.g. General Medical Council Confidentiality London, GMC (2009) and for an important discussion of the evolution of this area A.H. Ferguson, *Should a Doctor Tell? The Evolution of Medical Confidentiality in Britain* Ashgate (2013); G. Laurie, *Genetic Privacy* CUP (2002); see also J.V. McHale, *Medical Confidentiality and Legal Privilege* Routledge (1993) chapter 4.

2 See McHale, *supra* note 1, chapter 3.

3 This was still being experienced as a problem some two decades later. See A. Liu et al., 'Early Experiences Implementing Pre-exposure Prophylaxis (PrEP) for HIV Prevention in San Francisco' (4 March 2014) PLos Medicine http://journals.plos.org/plosmedicine/article?id=10.1371/journal.pmed.1001613.

discrimination in relation to HIV and AIDS has remained the subject of concern.[4] A further example is that of mental illness where such stigma and consequent discrimination remains to this day.[5]

Today we are in a new era of access to information, one where the internet has had a major impact. It can be argued that perceptions of individual confidentiality in an era of social media have changed out of all recognition. In a world where information exposure has increased, and where the level of information that is available about an individual has dramatically increased, is privacy now a devalued commodity? Yet many do value their privacy and see intrusion as a violation[6] and moreover some are prepared to forcefully assert it as the rise of so-called 'super injunctions' has grown experientially.[7] Furthermore, as some research has indicated while individuals may make use of social media that does not mean that they do not regard information control, privacy and confidentiality as being of importance.[8] In this uncertain world, how then does, and indeed should, the NHS address questions of privacy and of confidentiality?

Privacy itself as a concept – the right to be left alone – has been recognised only comparatively recently in law.[9] It is now safeguarded through international human rights declarations and through specific forms of protection that operate at state level. Privacy is rarely seen in absolute terms. So, while recognised in international rights statements such as Article 8 of the European Convention on Human Rights (ECHR), it is usually seen as a right qualified by reference to public interest considerations in issues such as national security, public health and the prevention of crime and disorder. English law gradually developed

4 R. Parker & P. Aggleton, 'HIV and AIDS-related stigma and discrimination: a conceptual framework and implications for action' (2003) 57(1) *Social Science and Medicine* 13.

5 E. Goffman, *Stigma: Notes on the Management of Spoiled Identity* (London: Penguin Books 1963). In relation to information sharing in mental health see further the Report of the Expert Committee Review of the Mental Health Act 1983 (1999) and J.V. McHale, 'Privacy and Confidentiality in Mental Health', in: L.O. Gostin, P. Bartlett, P. Fennell, J.V. McHale & R. McKay (eds.), *Principles of Mental Health Law and Policy* (Oxford: OUP 2010).

6 See for example the investigation into press ethics following the phone tapping investigation *The Leveson Inquiry, Culture Ethics and Practice of the Press Part I*: Report Published November 2012.

7 BBC News, 'BBC's Andrew Marr 'Embarrassed by Super injunction' 20 April 2011, www.bbc.co.uk/news/uk-13190424. The Independent News 'The worse kept secret is out: Jeremy Clarkson had an injunction', *The Independent*, 27 October 2011, www.independent.co.uk/news/media/press/the-worstkept-secret-is-out-jeremy-clarkson-had-an-injunction-2376453.html.

8 The Royal Academy of Engineering, *Privacy and prejudice: Young people's views on the development and use of Electronic Patient Records*', October 2010.

9 For the policy debates and ethical backdrop see the influential article by C. Warren & L. Brandeis, 'The Right to Privacy' (1890) 4 *Harvard Law Review* 193 and also in relation to the development of the concept C. Henkin, 'Privacy and Autonomy' (1974) *Columbia Law Review* 1742, A. Westin, *Privacy and Freedom* (New York: Athenum 1969).

to provide a framework for protecting confidential health care information. Common law developments in this area were reframed, through human rights principles and Article 8 of the ECHR, after the Human Rights Act came into force in October 2000. Moreover, additional safeguards were afforded through data protection legislation framed through the EU Data Protection Directive and now contained in the Data Protection Act 1998.[10] But despite such structures, there remain real concerns regarding the nature and scope of protection given to patient information.[11] At the same time steps are taken to make it easier for patient information to be accessed by third parties. So, for example, in August 2013 Geraint Lewis, Chief Data Officer of NHS England, announced that he wanted to cut the cost of access to data sets by companies from £20,000-30,000 to £1. Some six months later it was revealed that over 13 years of NHS data had been sold to insurance companies without patients' knowledge.[12] The utilisation of computerised systems such as care.data to store patient information has, as we shall see below, led to fresh challenges and fresh concerns.

This paper argues that health care confidentiality is today at a critical turning point; one where we have an opportunity to engage and frame individual rights and personal obligations but where, if we make the wrong choices, patient confidence and trust could be fatally undermined. Due to constraints of space its focus upon this is in the context of the use of patient information in the clinical context and also upon the adult patient. This paper begins by examining how the law concerning confidentiality and privacy safeguards health care information today. It outlines how confidentiality was very far from an absolute obligation right from the start and it explores the disconnect between perception and reality. Secondly, the paper explores recent developments concerning the NHS's own approach to the right to confidentiality and privacy and what this might mean in practice. Thirdly, it examines the major new patient records database care.data as a case study and the challenges this poses for the privacy and confidentiality of personal information. The paper concludes by suggesting that current developments both in relation to domestic and EU engagement with privacy issues may prove a real turning point, a valuable opportunity for patients to assert their rights and for policy makers to better confront countervailing disclosure considerations.

---

10 Directive 95/46/EC Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

11 'NHS lost 1.8 million patient records in a year', *Daily Telegraph*, 29 October 2012; 'NHS Surrey fined £200,000 after losing patients records', BBC News July 2013.

12 'Patient data should not have been sold, NHS admits', *Daily Telegraph* 24 February 2014 (13 years of NHS data sold to insurance companies), see also in relation to further examples M. Taylor, 'Health Research, Data Protection and the Public Interest in Notification' (2011) 19(2) *Medical Law Review* 267 at p. 268.

Safeguarding patient confidentiality from X v. Y and beyond

Legal protection for patient confidentiality emerged gradually, as with many areas of health care law, derived from a jurisdictional basis very far away from health care law itself. While there was evidence of the law restraining disclosure of medical information as far back as the eighteenth century in relation to the publication of the diaries of George III, it was rather the development of the equitable remedy of breach of confidence that provides the basis for the law in this area today.[13] This equitable remedy was originally developed to safeguard employer-employee confidential information. Initially there were three parts to the action. First, there needed to be information that had the necessary quality of confidence. Secondly, the information was disclosed in circumstances importing an obligation of confidence. Finally, the litigant had to show that there had been an unauthorised use of that information.[14]

Over time, the obligation was broadened. The case of *X v. Y* in 1987 crystallised the modern importance of the action in relation to health care confidentiality.[15] Here a national newspaper obtained information concerning two general practitioners who had AIDS. An action was brought using the equitable remedy of breach of confidence to stop further unauthorised disclosure of the information. The action was successful. It is interesting to reflect as to whether that case, which of course was decided at a time when a diagnosis of HIV and of AIDS was of particular sensitivity in relation to the adverse reaction and stigma that this could trigger, could be seen as a highpoint in protecting confidentiality in health care. After the Human Rights Act 1998 came into force in October 2000, the test for confidentiality was reframed. The European Court of Human Rights had already indicated that health care information could be safeguarded through a human right to privacy.[16] In *Campbell v. MGN*, the House of Lords had the opportunity to consider the application of the equitable remedy of breach of confidence post the Human Rights Act.[17] Here it was held that there were three critical issues for the court to consider. First, is there a reasonable expectation that the information is to be kept confidential? Secondly, would disclosure be 'highly offensive to a person of ordinary sensibilities'? Thirdly, is the infor-

13 *Wood v. Wyatt* cited in *Prince Albert v. Strange* (1849) 1 Mac and G 25.

14 *Attorney General v. Guardian Newspapers (No 2)* [1990] AC 109.

15 *X v. Y* [1988] 2 *All ER* 648: J.V. McHale, 'Doctors with AIDS Dilemmas of Confidentiality' (1988) 4 *Professional Negligence* 76.

16 *Z v. Finland* (1998) 25 *EHRR* 371; *MS v. Sweden* (1999) 28 *EHRR* 313.

17 [2004] 2 AC 457 HL, for discussion of the current law in the area see M. Brazier & E. Cave, *Medicine, Patients and the Law* (Oxford: OUP 5th edn 2011); J. Herring, *Medical Law and Ethics* (Oxford: OUP 2014); G. Laurie & J.K. Mason, *Mason and McCall Smith Law and Medical Ethics* (Oxford: OUP 2013).

mation 'obviously private'? In practice while there was a new test this did not change the essence of protection for health care professional-patient information, as Baroness Hale said in the *Campbell* case:

'It has always been accepted that information about a person's health and treatment for ill-health is both private and confidential. This stems not only from the confidentiality of the doctor-patient relationship but from the nature of the information itself.'[18]

Subsequently in *McKennitt v. Ash*, the Court of Appeal held that personal health information could be regarded as 'doubly private' where the information was disclosed in a relationship of confidence.[19]

The complexity of the relationship of confidentiality is highlighted by the role here of the NHS itself. The courts have confirmed that an obligation of confidentiality may be owed to the hospital in respect of the patient's medical records. Moreover while confidentiality had the practical effect of safeguarding patient information from disclosure, the ownership of patient records themselves was held by the relevant NHS body – such as the GP practice where the patient was being treated.[20] Thus from the onset there was what could be seen as a conflict. Confidentiality safeguarded disclosure but the control over that disclosure would not necessarily be in the hands of the patient – it could be seen as being concerned perhaps equally with paternalism in such situations as with respect for privacy and autonomy. Furthermore, health care confidentiality was simply not regarded as being absolute, nor indeed, it could be argued, should it be. Some information would be needed in practice to be passed on from one health care professional to another to ensure that a patient could be safely treated. Of course the precise extent to which such information disclosure was sanctioned, if known, could prove very surprising for a patient.[21] While patients may consent to information being disclosed and there will be no breach of confidence in the case of express or implied consent, considerable uncertainties remain as to the legitimate boundaries of such assumptions of consent, particularly in relation to implied consent.[22]

---

18 *Ibid*.

19 [2008] QB 73.

20 See further discussion below at page 116.

21 See further M. Siegler, 'Medical Confidentiality: a decrepit concept' (1982) *New England Journal of Medicine* 169.

22 See further discussion in G. Laurie & J.K. Mason, *Mason and McCall Smith Law and Medical Ethics*, 9th edn (Oxford: OUP 2013).

The test for confidentiality itself, as the courts have affirmed, is one of a balancing test between the public interest in confidentiality and the public interest in disclosure of information. Some judicial guidance has been given regarding what constitutes 'the public interest in disclosure'. Wood VC stated in *Gartside v. Outram* 'there is no confidence as to the disclosure of iniquity'.[23] Iniquity goes beyond, for example, the disclosure of information relating to a crime. It includes disclosure of information relating to 'matters medically dangerous to the public'.[24] Moreover disclosure of information must be in the public interest rather than simply being in the public interest to know.[25]

Even at what was perhaps the highpoint of the recognition of heath care professional confidentiality in the courtroom, there was a sharp reminder that health care confidentiality is by no means absolute. Just two years after the decision in *X v. Y* this was highlighted in the case of *W v. Egdell*.[26] Here W was held in a secure hospital after he shot and killed five people, wounding two others. He applied to a mental health review tribunal for a transfer or discharge and his solicitors commissioned a psychiatrist, Dr Edgell, to prepare a report in support of W's application. The report was unfavourable, suggesting that W had an abnormal personality that could be of a psychopathic nature and expressing concern in relation to W's interest in dangerous explosives. On receipt of the report, W's solicitors decided to withdraw his application from the tribunal and refused Dr Egdell's request for a copy of his report to be put in W's hospital file. Dr Edgell however disclosed the contents of the report to W's responsible medical officer and this report was also subsequently disclosed to the Home Office. W's case then arose for automatic review under the Mental Health Act. The report was produced at the hearing. W proceeded to seek an injunction and damages. In the Court of Appeal it was held that while W had a private interest in confidentiality, the true conflict was between the public's interest in confidentiality versus the public's broad, general interest in the disclosure. Nevertheless, on the facts of this particular case, disclosure was justified. The court was faced with a situation of an individual who had in the past committed multiple killings whilst seriously mentally ill and the decision related to whether a release decision would pose a sufficiently small risk. Bingham LJ stated:

'A consultant psychiatrist who becomes aware, even in the course of a confidential relationship, of information which leads him, in the exercise of what

---

23 *Gartside v. Outram* (1857) 26 L.J. Ch. (NS) 113, 114.

24 *Beloff v. Pressdram* [1973] 1 *All ER* 241, at p. 260, per Ungoed Thomas J.

25 *British Steel Corporation v. Granada TV* 1 *All ER* 435.

26 *W v. Egdell* [1990] 1 *All ER* 835: see J.V. McHale, 'Confidentiality: an absolute obligation?' (1989) 52 *Modern Law Review* 715; J.K. Mason, 'The Legal Aspects and Implications of Risk Assessment' (2000) 7 *Medical Law Review* 69.

the court considers a sound professional judgement, to fear that such decisions may be made on the basis of inadequate information and with a real risk of consequent danger to the public, is entitled to take such steps as are reasonable in all the circumstances to communicate the grounds of his concern to the responsible authorities.'[27]

Today the disclosure test itself now must be proportionate and thus in line with the Human Rights Act 1998.[28] Under Article 8(2), the interference with the right to privacy may be justified where 'in accordance with law and necessary in a democratic society' for those purposes as stated under the provision. These purposes include those of 'national security', 'public safety', 'prevention of disorder or crime', 'protection of health or morals' and 'protection of the rights and freedoms of others'. Such exceptions legitimate a range of situations in which confidentiality is delimited by statute, such as communicable diseases, road traffic accidents, and in accordance with court orders.[29]

Privacy can be used as a means of safeguarding personal health care information against disclosure. However, paradoxically, the cloak of privacy may also be used as a means of limiting individuals' control over their own personal information. This is through the recognition of the concept of anonymisation. It has been argued disclosure of information may be justifiable with the use of anonymisation because an individual is not identified and thus privacy is not infringed. This issue arose in *R v. Department of Health ex p Source Informatics Limited*.[30] The case concerned a company that wanted to collect information from pharmacists concerning the prescribing habits of general practitioners. Data collected included identity and quantity of the drug prescribed, and the GP's name. However, it did not collect the names of patients nor did it contain other identifying information. The Court of Appeal sanctioned this anonymised use of data for commercial purposes. They indicated that patients do not have any proprietary interest in the prescription form and if individual privacy interests were not put at risk, they had no right to control that information. The Court of Appeal saw the use of anonymised information as safeguarding a patients' privacy rather than putting it in peril. The decision in this case was unsurprisingly controversial. A distinction can be drawn between informational privacy issues, which may be safeguarded through anonymisation, and broader autonomy based issues concerning the control and use of information. Beyleveld and Pattinson have now argued that the interpretation in *Source Informatics* is

27 *Ibid*.
28 See *Campbell v. MGNsupra*.
29 See e.g. S. Michalowski, *Medical Confidentiality and Crime* (Ashgate: Dartmouth 2003).
30 [2000] 1 *All ER* 786 CA and see D. Beyleveld & E. Histed, 'Betrayal of Confidence in the Court of Appeal' (2000) *Medical Law International* 227.

narrower than both domestic and ECHR interpretations. They suggest that anonymisation itself would only be justifiable if it was in line with Article 8(2) of the ECHR, namely where it is 'necessary and proportionate for one of the stated interests'. In addition they also highlight the fact that in some instances the patient may have objections that fall within Article 9 of the ECHR the Convention right, which safeguards freedom of thought, conscience and belief.[31] A further important point in relation to anonymisation is made by Taylor, namely that there is a public interest in 'at least notifiying people what will happen to their data' and failure to do this can undermine 'public confidence in the ability of the system to take their interests into account'.[32]

If interpreted in this way by the courts, this would require a major reconsideration of the usage of patient information by researchers and other third parties in the future. However the traction from this judgment has very much impacted upon subsequent developments. From the highpoint of cases such as *X v. Y* and the Human Rights Act 1998 coming into force it can be argued that there has been effectively systematic erosion of privacy and confidentiality of health care information. A major shift in approach to exceptions to patient confidentiality developed from the early 2000s. Alongside the courts utilising human rights jurisprudence to facilitate protection of patient information, it can be argued that measures taken by the legislature have worked to systematically undermine this. First, this was triggered by concern in relation to the impact of the Data Protection Act 1998, particularly to the legality of holding clinical information in, for example, cancer registries and its use for clinical research purposes without further consent being obtained for such use. This led to the enactment of section 60 of the Health and Social Care Act 2001, now re-enacted as section 251 of the National Health Service Act 2006.[33] This provision enables the Secretary of State to make regulations providing for the processing of 'prescribed patient information for medical purposes as he considers necessary or expedient'. Such regulations may be made in the interests of providing patient care or in the public interest. Patient information can be disclosed under these regulations without consent, for example, in the context of communicable diseases and for other public health purposes.[34] Advice to the Secretary of State is provided by the Health and Social Care Information Centre (HSCIC), a statutory body established under section 252 of the Health and Social Care Act. These

31 D. Beyleveld & S. Pattinson, 'Confidentiality and Privacy', in: A. Grubb, J. Laing & J. McHale (eds.), *Principles of Medical Law* (OUP 2010).

32 *Supra* note 12 at p. 294.

33 Health Services (Control of Patient Information) Regulations 2002, SI 2002/1438, reg 4, and see also P. Case, 'Confidence Matters: The Rise and Fall of Informational Autonomy in Medical Law' (2003) 11 *Medical Law Review* 208-236.

34 SI, 2002/1438, s 3.

provisions have been controversial – some seeing them as a necessary means of facilitating research whilst others seeing them as enabling wide exceptions to the equitable remedy of breach of confidence. However, in retrospect this may be seen as merely a moderate step in the light of subsequent legislation. Today the Health and Social Care Information Centre also has further broad powers under the Health and Social Care Act 2012. Section 259 provides that it can require the provision of confidential health information from health professionals and 'any person (other than a public body) who provides health services, or adult social care, in England, pursuant to arrangements made with a public body exercising functions in connection with the provision of service of care'. It also has the power to require disclosure of information if this is necessary or expedient for its statutory functions to be performed. In relation to confidential information this can be disclosed in response to requests to collect information by the HSCIC or the Commissioning Board or if collection of that information is required by a person who has authority to do so.[35] Other information may lawfully be disclosed by request in some instances.[36] These are very wide powers indeed. Grace and Taylor argue that they mean that the 2002 regulations can be dispensed with and can be seen as further fundamentally undermining breach of confidence.[37] However as they have argued it can be said that the law does require that reasonable objection to the processing of personal confidential information should be respected.[38] It has been argued that this applies to both current and future disclosure.[39] The Information Governance Review stated that where objections are raised, the concerns should be addressed in line with both the NHS Constitution discussed below and the ECHR.[40] The objections should usually be respected but could be overruled under an 'alternative necessity'.[41]

Critically, confidentiality in clinical practice is today enshrined as a human rights obligation in law, but at the same time it is by no means absolute. There are also notable tensions and uncertainties as to its scope, not least, as we shall see in the following section, through the increasing retention of patient infor-

35 S 254-6 Health and Social Care Act 2012 and see J. Grace & M. Taylor, 'Disclosure of Confidential Patient Information and the Duty to Consult [2013] *Medical Law Review* 1.

36 See further s 257 Health and Social Care Act 2012 and Grace and Taylor *supra* note 35 at p. 19.

37 See further Grace and Taylor *supra* note 35 as to whether this can be seen as compatible with Human Rights and Data Protection law.

38 Discussed also in *The Information Governance Review*, 'Information: to share or not to share': *The Information Governance Review*, March 2013 at p. 79.

39 *Supra* note 38 at p. 82.

40 *Supra* note 38 at p. 79.

41 This would include, according to the review, emergencies under the Civil Contingency Act 2004, health protection and even sometimes potentially under s 251, e.g for research into child abuse see note 37 *supra* at p. 81.

mation on databases and the powers of bodies such as the HSCIC. In the next section we explore how the NHS itself views privacy and confidentiality in the context of patient information today and address some uncertainties that remain.

Confidentiality, privacy: the NHS Constitution and information governance

Confidentiality and privacy is enshrined in the commitments made by the NHS. The NHS Constitution, which is a statement of rights and pledges in the NHS, provides that:

'You have the right to privacy and confidentiality and to expect the NHS to keep your confidential information safe and secure.

You have the right to be informed about how your information is used.

You have the right to request that your confidential information is not used beyond your own care and treatment and to have your objections considered, and where your wishes cannot be followed, to be told the reasons including the legal basis.'[42]

The extent to which the NHS Constitution creates new rights or simply restates existing rights may be questioned. It is of course the case, as we saw above, that privacy and confidentiality are already protected in English law. Thus in this respect the NHS Constitution is simply restating an existing right. The right to be informed in relation to use of information can be seen as a 'new right' but this also flows from obligations concerning data protection law. Moreover, it is unclear how this relates to the pledges contained in the Constitution, which are explored below. A further confusing aspect here relates to disclosure in the public interest. In law there is no necessary right to be informed in relation to disclosure of information where a person is, for example, posing an immediate risk of harm to another. The provision that refers to a right to request that information is not used for other purposes does not constitute a right to patient privacy in the sense of decision-making autonomy. Moreover the section on rights does not engage with whose information this is that of patient or that of the NHS itself and indeed *who* should have such control powers.

The NHS Constitution is also not simply concerned with 'rights' but it also makes reference to a range of what are termed 'pledges'. The Constitution states that:

---

42 NHS Constitution (2013), www.nhs.uk/choiceintheNHS/Rightsandpledges/NHSConstitution/Pages/Overview.aspx.

'The NHS also commits:
- to ensure those involved in your care and treatment have access to your health information so they can care for you safely and effectively (pledge);
- to anonymise the information collected during the course of your treatment and use it to support research and improve care for others (pledge);
- where identifiable information has to be used, to give you the chance to object wherever possible (pledge);
- to inform you of research studies in which you may be eligible to participate (pledge); and
- to share with you any correspondence sent between clinicians about your care (pledge).'

The first pledge seems to make the assumption that data disclosure will be facilitated. This is particularly interesting in the light of the care.data discussion, which we shall return to shortly. What this precisely means is unclear. What information will really be needed to care 'safely and effectively' for a patient? The statement on anonymisation and use of information for research restates first the approach from *Source Informatics*, and secondly, existing practice concerned with data protection and research use of information. But again this makes the huge assumption that anonymisation rather than respect for personal decision-making autonomy is key. Moreover, it makes the further assumption that individuals will necessarily agree with the use of that information for research purposes and indeed agree with a particular type of research. Again, views on the validity and acceptability of different research practices may vary radically. The aim of enabling someone to object wherever possible where identifiable information is used again depends critically on what is meant by 'wherever possible' and the means used to facilitate this. It is also interesting that these pledges appear immediately before a pledge to inform people on research projects in which they may participate.

The uncertainties in relation to the use and sharing of information was highlighted by the NHS Futures Forum, a body established by the Government to scrutinise the impact of the Health and Social Care Bill (now the Health and Social Care Act 2012).[43] In June 2012, the Government also produced a White Paper, 'Open Data: Unleashing the Potential'.[44] This stressed the aim both that 'data that can be published should be published' and that it was intended that it would 'safeguard people's data from misuse and rigourously protect the public's right to privacy'.[45] The Government had meanwhile established an In-

43 *Information*, a Report from the NHS Futures Forum, January 2012.
44 Cabinet Office, June 2012.
45 *Ibid*.

formation Governance Review following the NHS Futures Forum in 2012, chaired by Dame Fiona Caldicott, which reported in March 2013.[46] Dr Caldicott's very important report in the 1990s led to the establishment of the Caldicott principles in relation to information sharing in the NHS.[47] Dr Caldicott has also now been appointed as the National Information Guardian to provide oversight.[48] Here we focus upon some of the key recommendations of the Review as these relate to confidentiality and privacy of personal health information. At the heart of the Information Governance Review was a restatement of these original Calidcott principles.[49] These now provide that the first principle is that of justifying the purpose with 'clearly defined scrutinised and documented transfer of data'. Secondly, confidential information should not be used unless 'absolutely necessary'. Thirdly there should be the use of the minimum necessary of confidential data. Fourthly, information access should be on a 'need to know basis'. Fifthly, 'everyone with access to personal confidential data should be aware of their responsibilities'. Sixthly, where such material is used the use should be lawful. Finally, the principles state that 'the duty to share information can be as important as the duty to protect confidentiality.'

The Information Governance Review highlighted individuals' right to access personal information.[50] As we have seen, anonymisation and de-identification have been regarded in the past as a means of providing safeguards. One major problem here concerns the question of linkage. In the context of research there has been considerable advocacy of the use of so-called 'safe havens'. The Information Governance Review held that if there was linkage of personal confidential information or data that was de-identified but there was still a considerable risk that it could lead to re-identification, then, in such a situation, the linkage should only take place in 'specialist well-governed, independently scrutinised and accredited environments called 'accredited safe havens'.[51] The HSCIC (discussed further below) is one such 'safe haven' under the Health and Social Care Act 2012 where confidential information can be collected and identified but without the risk of disclosure of individual confidential data. In addition, the criteria for the operation of further such safe havens was to be set out in codes produced by the HSCIC and moreover advice given by the Information Services Commis-

46 *Supra*.
47 *The Report on the Review of Patient Identifiable Information* (The Caldicott Report), 1997.
48 'National Data Guardian Appointed to Safeguard Health Information', Department of Health, News story, 13 November 2014, www.gov.uk/government/news/national-data-guardian-appointed-to-safeguard-patients-healthcare-information.
49 *Supra* note 38 at p. 118.
50 *Supra* note 38 at p. 29.
51 *Supra* note 38 at p. 66, see also R. Thomas & M. Walport, *Data Sharing Review* July 2008, http://systems.hscic.gov.uk/infogov/links/datasharingreview.pdf/view.

sioning Group to the Secretary of State should set out procedures in relation to, for example, granting accredited status.

The Review stated that health information sharing was permissible by email, where individuals had expressly consented and were informed of the potential risk.[52] The Review held that 'relevant personal confidential information' could be shared amongst health and care professionals who have a 'legitimate relationship with that individual'.[53] It stressed the importance of an audit trail detailing everyone who has had access to individual electronic confidential data that should be made available to patients.[54] This is an excellent recommendation that will facilitate transparency and openness. Consent should be obtained before the sharing of whole records concerning health and social care with other health care professionals and exceptions here needed to be based on professional judgement.[55] The care team is intended to include registered social care professionals.[56] 'Robust' sharing arrangements should be put in place in relation to those health and care staff providing direct care who are not registered with a regulatory authority.[57] This is clearly critically important given the increasing use of such staff. The Report stated that there was limited awareness of the nature of implied consent and it sought to try to clarify this and importantly emphasised that this was only applicable in relation to direct care.[58] In relation to the use and sharing of personal and confidential information, the Information Governance Review Panel said that, while it was not deficient in itself, nonetheless it was recognised that there could be improvements in communication to patients and to staff. It suggested that existing consent arrangements did not need to be redesigned, rather that:

'All organisations in the health and social care system should clearly explain to patients and the public how the personal information they collect could be used in a de-identified form for research audit, public health and other purposes. All organisations must also make clear what rights the individual has open to them including any ability to actively dissent (i.e. withhold their consent).'[59]

Also in relation to consent, the Review stated that the Information Services Commissioning Group of the NHS should develop or otherwise commission

52 *Supra* note 38 at p. 30.
53 *Supra* note 38 at p. 38.
54 *Supra* note 38 at p. 33.
55 *Supra* note 38 at p. 38.
56 *Supra* note 38 at p. 39.
57 *Supra* note 38 at p. 41.
58 *Supra* note 38 at p. 36.
59 *Supra* note 38 at p. 57.

guidance for recording information regarding decisions concerning information sharing and a strategy concerning how this information could be shared and wishes protected. The Review noted that the need to ensure compliance with the Directive meant that reasonable expectations were to be respected.[60] However it then goes on to say that 'reasonable objections from individuals must be considered' – which is something rather different.[61] Individuals were to be given as much information as possible to make a decision – but that is not to say that this will be Human Rights Act compliant. The Review suggests a series of criteria such that the process for considering objections should include the most senior health care professional caring for the patient, whether agreeing to the objection should damage effectiveness of care and whether there was a risk that safety of the patient would be reduced by not upholding the patients' decision.

In relation to withdrawal of consent, the Review highlights that consent should be reviewed where someone decides to remove consent. It then goes onto state that 'withdrawal of consent cannot be reliably made retrospectively', and, referring to other guidance, that it is not advisable to delete records and information and that an audit trail is needed in relation to the removal of electronic records. This is a difficult issue. On the one hand, an audit trail can be seen as practically important and advantageous to the institution. At the same time such restrictions may be seen as going entirely against the notion of autonomous control of information. Yes, it may be problematic but this precisely hits at the question of *whose* information it is. It is disappointing that this was not one of the key points of the Review's discussion. Data breaches were considered in the report, as was the need to ensure that there was a scale in relation to severity of breaches that was agreed across the NHS to facilitate consistency.[62]

The case of care.data

There has long been tension between control and ownership of patient information in the NHS. Patient information has been routinely recorded in the NHS since 1911 with the so-called 'Lloyd George' record.[63] Initially patients could not access such records themselves, although access could be obtained if needed in the context of litigation.[64] There was a considerable battle

60 *Supra* note 38 at p. 78.
61 *Supra* note 38 at p. 79.
62 *Supra* note 38 at p. 54.
63 See further Nuffield Council on Bioethics Report*: Biological and Health Data Ethical Issues*, Nuffield Council on Bioethics, London, 2015 at p. 7.
64 See Supreme Court Act 1981, s 34.

before statutory patient access was gradually allowed in the late 1980s and early 1990s.[65] The Data Protection Act 1984, which gave an initial right of access to computerised records, can be seen as a catalyst for change. The Access to Medical Reports Act in 1988 gave a statutory right of access to medical records compiled for insurance and employment purposes. The Department of Health at that time was of the view that records were the property of health authorities, with general practice records being owned by the Family Health Service Authorities. As technology developed, paper records were eventually replaced with computerised records in 2011.[66] The use of computerised medical records led to concerns as to its impact on patient confidentiality. This was followed by the Caldicott Report, establishing principles of information governance. Interestingly, as Nuffield noted, by the time of the second Caldicott Report there was a shift in approach from concern with failures to protect data to instead promoting 'a culture of responsible data sharing'.[67] It is in this context that we need to consider the development of care.data.

The backdrop to the development of care.data can be seen in the introduction of the Summary Care Record by the Labour Government, rolled out in England in 2010. This scheme involved the development of new IT systems across the NHS. This was continued by the Conservative/Liberal Democrat Coalition Government when it took office. The scheme was intended to initially contain a summary of patient information from the GP system and in addition some hospital referral and discharge correspondence other than clinical details.[68] Subsequently it was to incorporate what were known as the Common Assessment Framework plan documents – the intention here was to facilitate joint health and social care provision. However, from the start there were problems in relation to its implementation through complexities concerning the technical issues of its operation as well as policy questions.[69] A review of the scheme found that it had not been successful; it had been little used for example, by medical professionals working in Accident and Emergency departments.[70] In addition, entry into the scheme was by 'opt-out'. Interestingly not only did a significant number of persons opt out, but criticisms were also made that there was inadequate information in relation to how individuals should opt out. Ultimately, in 2013, the National Programme for IT (NPfIT), described as 'the largest

65 See for example, a cautious judicial approach *in R v. Mid Glamorgan Family Health Services Authority ex parte Martin* [1995] 1 *All ER* 356 and for discussion of some of the concerns regarding access see M. Gilhooley & S.M. McGhee, 'Medical Records, practicalities and principles of patient possession' (1991) 17 *Journal of Medical Ethics* 138.

66 *Ibid*.

67 *Supra* note 63 at p. 38.

68 *Ibid*.

69 *Supra* note 63 at p. 104.

70 *Supra* note 63 at p. 105.

ever civilian IT project failure in human history', was abandoned.[71] As the Nuffield Council on Bioethics have highlighted,

'the experience of the NPfIT may, nevertheless, be salutary for health care data initiatives more generally because it highlights the risks of external drivers overtaking the establishment of data initiatives ... and of lack of involvement or imbalance of key interests and the need adequately to address values and norms relating to confidentiality'.[72]

The Health and Social Care Information Centre is a non-departmental public body created in 2012 by the Health and Social Care Act 2012. It succeeded an earlier body, the NHS Information Centre, and was intended to provide a 'safe haven' in relation to health data. A quarter of the data held concerns health, the rest concerns social care. It collects information from health and social care bodies; it then holds it within a suitably secure environment and moreover may 'make that information readily available for others to turn into 'actionable business intelligence.'[73] One major project to collate information that is collected routinely by the HSCIC is the care.data project.[74] This is concerned with collating data from primary care and increased secondary – hospital care data. It was presented as an extension to existing schemes, but in fact the extent to which that is the case depends, as the Nuffield Council on Bioethics has highlighted, on the robustness of previous data collection schemes, which had been criticised in relation to their operation. Information extracted electronically through GP practices, while not including names of patients, will include their NHS number, date of birth and postcode, as well as diagnoses, prescriptions and other procedures such as vaccinations. Pseudonymisation will be undertaken before the information is made available to bigger data sets, however it has been confirmed that there is the possibility that re-identification could take place and where such information is made available to researchers they must sign legally binding agreements to acknowledge such risks.[75] The further aim is to link care.data to other data such as genomic data being extracted under the 100K Genome Project, which is being run by Genomics England.[76]

---

71 *Supra* note 63 at p. 105.

72 *Supra* note 63 at p. 106.

73 Health and Social Care Information Centre, *Exploiting the potential of health and care data*, London: HCIC (2012).

74 J. Hoeksma, 'The NHS care.data scheme: what are the risks to privacy' (2014) 348 *BMJ* 1136 and see also for a broader discussion of the relationship between this project and research in P. Carter, G. Laurie & M. Dixon-Woods, 'The social licence for research: why care.data ran into trouble' (2015) *Journal of Medical Ethics* online first, 25 January.

75 *Ibid.*

76 www.genomicsengland.co.uk/.

The first major problem with the project related to consent. Reasonable notice is required under the Data Protection Act 1998 to be given to the data subject as to how information should be used.[77] NHS England stated in August 2013 that GPs had the responsibility of informing patients that the data would be used in this way.[78] However, it was subsequently considered that this would be burdensome and a leaflet was distributed to homes setting out the scheme and the provisions concerning 'opt-out'. Criticism as to the operation of the scheme led to it being halted when it became clear that individuals had not received leaflets, did not understand the implications of the leaflets, or were having problems opting out. As the Nuffield Council on Bioethics Report *Biological and Health Data: Ethical Issues* noted, general practitioners in England were placed in a difficult position in that under the Health and Social Care Act 2012 they were compelled to submit data to the HSCIC but at the same time they also had to comply with Data Protection Act principles and moreover this was fundamentally confidential patient information.[79] In contrast in Scotland and in Wales general practitioners themselves were not compelled to be involved in the database.[80] The Nuffield Council have argued that 'questions about the terms under which information may be collected and disclosed by the HSCIC need to be answered by first establishing the norms of access and disclosure that govern the kinds of information transactions involved'.[81]

The operation of the care.data scheme was also considered further in a report by the All Party Parliamentary Group (APPG) for Patient and Public Involvement in Health and Social Care published in November 2014.[82] It was noted that there had been strong support in response to the APPG from certain respondents for the advantages of sharing data to facilitate research purposes that could facilitate the performance of NHS services.[83] However, various aspects of the scheme attracted particular comment from the APPG. First, whether it should be 'opt-in' or, as at present, patients should have to 'opt out' of the system. There was some support for opt-out from professional groups and charities who responded to the consultation. Opt-in is time-consuming and it can be problematic trying to ensure that individuals actually make a decision. Furthermore, it could have an adverse impact upon data sets if it is later sought to use these for

77 See discussion in Taylor and Grace *supra* note 35.
78 *Supra* note.
79 *Supra* note 63 at p. 109.
80 M. McCartney, 'Care.data, why are Scotland and Wales doing it differently?' (2014) 348 *BMJ* 1134.
81 *Supra* note 63 at p. 108.
82 *The All Party Parliamentary Group for Patient and Public Involvement in Health and Social Care Care.data Inquiry Report*, November 2014.
83 *Supra* note 72 at p. 23.

research purposes. While these concerns were recognised, the APPG commented that:

'in order to ensure sufficient numbers consent on an "opt-out" basis for their data to be collected, and for the data extraction to be legitimate and ethical, the programme must be properly explained, so that patients understand their rights, their choices, the potential benefits, and so that any concerns are answered.'[84]

It is interesting that a very different approach has been taken in Wales where no fully identifiable patient information is held and any attempt to access such data can only be with individual patient consent.[85]

The APPG welcomed moves to pilot this via GP practices. They also indicated that there could be a means for GP practices to facilitate the opt-in/out process and make it easier. It was suggested that there should be steps to ensure that records were accurate and that processes were in place to ensure that individuals knew how records were being shared. It was also concerned to emphasise the need for 'robust safeguards in the IT systems' to stop unauthorised access of information. Moreover, it suggested that the current method of implementation could be seen as being inconsistent with the NHS Constitution. The APPG did not respond to this point in its findings in the Report. In addition what opt-out really meant was something that needed to be highlighted, as if an individual 'opted out' data would still be held but in an aggregated form. Where opting out was available in the past, its implementation in practice had proved problematic in some cases as highlighted in evidence to the APPG from the Patients' Association.

Further objections were also raised by the Alzheimer's Disease Society in evidence in relation to how the existing law applied concerning confidentiality. It was suggested that although some opt-outs might be justifiable, examples given were strict purpose limitation on the transfer and re-use of data, proper governance, an audit of uses, and also strict penalties for incorrect data use or identification of individuals, other uses might be problematic. The APPG Report noted concern that onward transfer of data, for uses that have no direct link to health care and no advantage for patients, could constitute an unjustified breach of the obligation of patient confidentiality required by English law. This issue was not explored further by the APPG in its conclusions but remains a fundamentally important question.

---

84 *Supra* note 82 at p. 24.
85 *Supra* note 82.

The second and related problem here, which appears not to have been raised when the scheme was being planned and initially implemented, concerns the question of adults who have diminished or diminishing mental capacity. This was highlighted in responses to the APPG by the Alzheimer's Disease Society. As it noted, section one of the Mental Capacity Act 2005 provides a statutory presumption of capacity. Nonetheless, while some patients with dementia may be able to make a decision in relation to the use of their data, the test for capacity, as set out in that legislation, is a decision-relative test, and some patients may not be able to do so. The Alzheimer's Disease Society called upon the Government to obtain legal advice concerning the Mental Capacity Act and the 'opt-out' policy of the care.data programme. The Society noted that it had not been receiving calls about the care.data project, which suggested that public understanding in relation to this was low. This is an extremely important issue and the lack of its effective consideration by the Government in relation to the introduction of the scheme represents a glaring omission. What was also notable in relation to the responses to the APPG was the consistent criticism of the lack of consultation in relation to the introduction of the scheme by a range of respondents, and this was highlighted in the APPG's Report.[86]

A third major problem with the care.data scheme relates to the scope of sharing of information. Exactly how will this information be used? Such collated data is valuable and could have considerable commercial significance. The APPG Report also commented that 'its use should be restricted to the agreed purpose for which it is being shared'. The Report identified strong opposition to other uses. For example, the National Association for Palliative Care indicated its concerns in relation to the information being made available to commercial organisations and how this could be used as a means of marketing to vulnerable groups.[87] As the APPG commented, there is considerable public concern in relation to access by insurers and others to such data. In relation to subsequent use of the data, the Report recognised that it may be attractive to commercial organisations.

'The current information around the legislation is worded as individual-level data not being eligible for release unless there is a clear health or care benefit for people. It is not outside the realms of possibility that a commercial enterprise could make a case for benefit in order to gain access to data, but there is no information about how the use of data would be monitored and whether the benefit would need to be proved in order to maintain access to the data. Further guidance on this would be welcome.'[88]

---

86 *Supra* note 82 at p. 8.
87 *Supra* note 82 at p. 8.
88 *Supra* note 82 at p. 25.

Use of health care records after death was also highlighted as a concern in evidence to the APPG. In law, the extent to which an obligation of confidence extends after death still remains uncertain. Initially it was thought that, analogous with defamation, the obligation would not apply after decease. However, for many years, professional ethical codes took the approach that it does apply.[89] In *Lewis v. Secretary of State for Health*, Foskett J held obiter that 'it is arguable that the duty of confidentiality does survive the death of the patient' (in this case both parties had accepted that the obligation had continued).[90] It was unclear as to how such information stored in care.data will be dealt with after a person has died and whether this information will be made available to other organisations. The whole question of use of patient information after death remains a source of discussion. The Information Governance Review also considered this point and hoped the Law Commission would give consideration to this, for example by the prospect of the transfer of custodianship of information through an individual's last will and testament.[91]

The project is being taken forward through working with targeted GP practices developing communication materials and working, for example, on the use of emails and text messages as well as leaflets. This will be overseen by Dame Fiona Caldicott and it is intended it should be evaluated before being rolled out nationally.[92] It is clear, however, that important issues raised by the APPG remain to be fully addressed. The developments concerning care.data illustrate that huge challenges and tensions remain concerning privacy, confidentiality and broader public interest considerations in relation to the use and disclosure of patient information – but perhaps also opportunities. We explore these further in the concluding section.

Conclusions

A golden age of health care confidentiality can be overstated. In reality, as we have seen, confidentiality has always been a very leaky sieve – confidentiality often subject to a balancing text and undermined by a myriad of statutory exceptions. Nonetheless, from arguably a 'high point' of respect for health care information through the courts in *X v. Y* and in the NHS itself,

89 See e.g. in relation to Winston Churchill, S. Lock & J. Loudan, 'A Question of Confidence' (1984) 288 *BMJ* 123 and in relation to publication of details concerning President Mitterrand, A. Dorozynski, 'Mitterand Book Provokes Storm in France' (1996) 312 *BMJ* 201 *Plon (Societe) v. France* Application No 58148/00 18 May 2004.

90 [2008] *EWHC* 2196.

91 *Supra* note 38 at p. 69.

92 NHS *The Care.data Listening, Exercise and Action Plan*, NHS December 2014, www.england.nhs.uk/wp-content/uploads/2015/01/care-data-presentation.pdf.

through the very first Caldicott report in 1997 signalling concern around the prospect of the threat to confidentiality and privacy in relation to patient information today, we are now clearly at a very difficult time in relation to the safeguarding of patient information. Evolving models of clinical practice provide new challenges. The re-structuring of NHS care may impact upon a patient's perceptions of confidentiality. The reality of a health care professional-layperson consultation is that, frequently, individuals may not see their own GP. Rather, they will have to consult the GP on duty on that day who may be a partner, an associate, a locum or, if after 6pm, part of a contracted out-of-hours service. Thus there is broader access to information about a patient – and rarely is patient care within a simple and single doctor-patient relationship throughout a patient's life.

There is a public perception that respect for individual privacy and confidentiality has been eroded as clearly demonstrated by the major problems with the implementation of the care.data project. At the time of writing, the project is being driven ahead. It is assumed that privacy safeguards are in place – yet it remains highly questionable as to whether an individual right to autonomy in relation to control of access to information is being safeguarded. The debate over care.data can be seen in terms of questions of practicality. It is not feasible to ask everyone to opt in. They simply will not respond; perhaps they will not understand; they might even say no; and, of course, if large numbers of patients did this, the whole project would crash. There are resonances here with the debate in the 1980s, alluded to earlier, concerning patients' access to their records. Numerous arguments were put forward before the introduction of the Access to Patients Records Act in 1990 as to why it would be problematic/wrong/dangerous to let patients get hold of their own medical records. Ultimately, when a right of access was allowed, the portents proved unrealistic. It could be seen as a means of facilitating patient-clinician partnership. Care.data can perhaps be seen in a similar way. By truly engaging with individuals, allowing them to make decisions then the scheme is likely to be a success. For patients to retrospectively discover the nature and scope of information disclosure, which, they argue, they have not been properly informed about, is likely to prove exceedingly problematic, as the initial implementation of the scheme demonstrates. In addition, it can be seen as an infringement of individual human rights and, of course, yet another hugely damaging reputational incident. However, in contrast, if such steps lead to proper patient access to information online, this could be hugely empowering. Patients could truly monitor their care, including who has access to their online information, as the Information Governance Review has suggested. Currently, patients have to totally opt in or opt out. It has been suggested that a better approach would be to enable selective

opt-in and opt-out of use of patient information for specific functions.[93] Such an approach would much better enable public confidence and proper engagement and respect for both privacy and confidentiality of personal information. What is clear is that certain legal uncertainties still have to be resolved. First, the question of the involvement of records of adults with diminishing mental capacity as noted in the APPG Report, and secondly, use of medical information from the deceased as highlighted both in the Information Governance Review and by the APPG.

The taking forward of care.data does have the consequence of highlighting a further disparity in relation to the safeguards given to personal health information. If care and treatment is entirely outside the NHS, through the use of private GPs and private hospital care, an individual would be able to circumvent the system entirely and maintain far greater control of their own personal information, which would be excluded from research purposes and suchlike, unless the individual directly consented to its inclusion. It would be of concern if the strength of individual privacy rights in relation to health care information may in the future simply come down to financial resources to control access to care. Moreover, as the interface between private care and NHS provision in general becomes blurred, to what extent can and indeed should information within the NHS be seen truly as a 'public resource' for future use?

We are perhaps at a critical turning point in another respect through movements at EU level and the gradual evolution of a 'right to be forgotten'. This issue reached public attention through attempts by individuals to remove information concerning them that was available through internet search engines in the case of *Google Spain v. Agencia Espanola de Proteccion de Datos*.[94] Here Costeja Gonzalez, a Spanish resident, lodged a complaint against a Spanish newspaper and Google that if a person used the internet search engine it would provide a link to newspaper article of 19 January and 9 March 1998 that concerned an announcement for a real estate auction in relation to proceedings for recovery of social security debts and he asked for personal data concerning him to be removed. The European Court of Justice considered this application in the context of the EU Data Protection Directive 95/46/EC and the EU Charter of Fundamental Rights and Freedoms. Both these documents make reference to protection of the right of the individual to privacy. This is a particular issue given the nature and the scope of the application of search engines. While internet search engine users may have legitimate interests in relation to access

93 D. Shaw, 'Care.data consent and confidentiality' (2014) 384 *Lancet* 1207.

94 Case C-131/12, *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González*.

to such information, this needs to be balanced against the rights of the individual. Moreover, as the ECJ stated, this may depend upon the nature of the information and also its sensitivity for the individual's private life and the broader public interest in access to such information. In addition, there was no need to obtain removal from the individual websites themselves first, as this can be problematic in practice given the ease of replication of information on websites. The very fact that information is included on a search engine the ECJ held, was a more significant interference with privacy than inclusion on the website. The question of the 'right to be forgotten' had already formed part of the discussion in relation to the reform of the EU Data Protection Directive. This is currently subject to reform through the consideration of a new regulation.[95] Included in the original proposal for the legislation was an article addressing the right to be forgotten. This proved extremely controversial. The proposal was being discussed at the time when the *Google* litigation was ongoing. The ultimate Regulation produced by the EU was more restrictive. Instead of referring to a 'right to be forgotten' it now uses the language of 'a right to erasure'. Article 17 provides that a data subject can ask for data to be removed on a series of grounds. These include circumstances in which the controller's legitimate interests are overridden by interests, or fundamental rights or freedoms, of the data subject(s). The Regulation also allows for erasure of links where the data has been made public. Nonetheless this right does not apply to freedom of expression rights, public interest rights in the area of public health or for historical, statistical or scientific research purposes, or in a situation in which it is required for compliance with a legal obligation to retain the personal data by Member State law. While the right itself will thus be limited, its very existence, its profile and the rhetoric around it have already caused considerable debate. To date much of this has centred around the free speech aspects of the *Google Spain* case, but, longer term, other implications remain to be considered, including the extent to which recognition of such rights may seek to redefine how we approach questions of informational privacy. This has major implications for safeguards for individual patient confidentiality and privacy. What if an individual wants part of their information erased because it could have subsequent damaging career and insurance aspects if it were retained on file? Furthermore, an individual might object to their information be utilised by researchers subsequently and want information that may be of considerable utility to the researchers deleted.

The discourse around the right to be forgotten is very different and if this is taken further in the future it may lead to much re-conceptualisation in this

95 Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Brussels 25.1.2012 COM(2012)11 final SEC (2012)72 final.

area. It relates to the ability of individuals to control their information, to eradicate past traces and to determine privacy, autonomy and identity. At a practical level there is also much that needs to be done to take forward real engagement with privacy and autonomy in health care. Perhaps establishing an NHS National Information Guardian and regulatory oversight through the Health and Social Care Information Centre is not enough. There is need for detailed engagement too with health care professionals themselves concerning these issues. As the Information Governance Review highlighted, the provision of annual training on information governance was viewed by staff as akin to an 'annual sheep dip', which staff went through without thinking.[96] As the Review rightly notes, there needs to be thought, real reflection and understanding, but, moreover, the importance of information governance and information sharing be incorporated in professional training and re-validation.[97] It states that there is a need for all organisations that process personal confidential data including local authorities, social care, telephony and other social care providers, to appoint Caldicott guardians.[98]

There are broader policy questions in relation to privacy, confidentiality and patient information that arise here. The Nuffield Council on Bioethics Report suggests that there was a moral question here for the NHS and for the HSCIC, namely to 'define a public set of morally reasonable expectations about the use of data generated by health and social care'. These need to be within a principled framework taking into account private and public interests.[99] The Report comments that use of data should first have expectations that are 'grounded in the principle of respect for persons'. In addition such expectations should flow from established human rights. Thirdly, such expectations and the determination as to how these will be met should be with participation from those persons who have 'morally relevant interests'. Finally, there need to be effective modes of governance and accountability and these include structures of accountability both in the form of judicial and political authority but also interestingly through what it terms 'social accountability arising from engagement of people in society.' These are important, thorough and well-timed statements. There is much further work that would need to be done as to how this could be taken forward in the NHS. There remains, however, a very big question as to whether such matters can and should be left simply to the NHS. There are clearly broader issues concerning Big Data and data sharing that impinge here. In relation to

96 *Supra* note 38 at p. 89.
97 *Supra* note 38 at p. 90.
98 *Supra* note 38 at p. 92.
99 *Supra* note 63 at page 112.

the use of data more generally, the Law Commission, in a major report published last year, has recommended that:

'A full law reform project should be carried out in order to create a principled and clear legal structure for data sharing, which will meet the needs of society. These needs include efficient and effective government, the delivery of public services and the protection of privacy. Data sharing law must accord with emerging European law and cope with technological advances. The project should include work to map, modernise, simplify and clarify the statutory provisions that permit and control data sharing and review the common law'.[100]

This recommendation is clearly timely. But such proposals and reform of the law in this area will inevitably be a huge task. Such developments also suggest that we really are now at a critical turning point in relation to the privacy and confidentiality of health care information and its relationship with other information. Moreover, this discussion is also pertinent as the General Medical Council at the time of writing is reviewing its guidance on confidentiality.[101] The time has come to move from a focus on unauthorised disclosure to return to first principles and reframing this area in terms of patients' rights and patient autonomy – to truly fuse respect for privacy, both informational and autonomous. There have been attempts to align public interests in disclosure with those of privacy in relation to specific areas such as genetic data[102] – but there is a need now for a return to a broader re-evaluation of confidentiality and privacy and of data sharing as we move into what may become a new era of patient rights to autonomy, privacy and, perhaps, also a right to be forgotten.

---

100 Law Commission, *Data Sharing Between Public Bodies* (2014), http://lawcommission.justice.gov.uk/areas/data-sharing.htm.

101 See further www.gmc-uk.org/guidance/news_consultation/25893.asp.

102 See for example the incisive elegant analysis by Mark Taylor, in: *Genetic Data and the Law: A Critical Perspective on Privacy Protection* (CUP 2012).