BRILL
NIJHOFF

EUROPEAN JOURNAL OF HEALTH LAW 29 (2022) 1–12

European Journal of Health Law

brill.com/ejhl

Information Privacy in Healthcare — The Vital Role of Informed Consent

Roy McClelland
Faculty of Medicine Health and Life Sciences, Queen's University Belfast, University Road, Belfast BT7 1NN, Northern Ireland, UK

Colin M. Harper | ORCID 0000-0003-2503-0460
Department of Social Policy, Queen's University Belfast, 69–71 University Street, Belfast BT7 1HL, Northern Ireland, UK
Corresponding author, e-mail: colin.harper@qub.ac.uk

Abstract

The use and disclosure of patient information is subject to multiple legal and ethical obligations. Within European human rights law the differences relating to consent are reflected in the separate requirements of data protection law, the common law, and professional ethics. The GDPR requires explicit consent. This contrasts with the ethical and common law availability of reliance on implied consent for the use of patient information for that patient's care and treatment. For any proposed use of patient information for healthcare purposes other than direct care, even where GDPR may be satisfied if the patient refuses to consent to disclosure, the information should not normally be disclosed. For any proposed use or disclosure outside healthcare the justification should normally be consent. However, consent is often not possible or appropriate and an overriding public interest can be relied upon to justify the use or disclosure, both legally and ethically.

Keywords

confidentiality – privacy – data protection – consent – healthcare – Europe

1 Introduction

Privacy is recognised as a fundamental human right.[1] In healthcare settings the right to privacy has effect in many ways, including in the sharing of information provided by patients for their healthcare. The Council of Europe has emphasised the importance of respecting the privacy of health data. This is recognised as a central principle in the legal systems of all the Contracting Parties to the European Convention on Human Rights (ECHR).

> It is crucial not only to respect the privacy of a patient, but also to preserve his or her confidence in the medical profession and in the health services in general. Without such protection, those in need of medical assistance may be deterred from revealing such information of a personal and intimate nature as may be necessary in order to receive appropriate treatment and, even, from seeking such assistance.[2]

There is no general requirement in the European Convention on Human Rights (ECHR) that disclosure of personal health information requires consent, but any such disclosure must serve at least one of a defined range of public interests.[3] The European Union Charter of Fundamental Rights rests on the ECHR but goes further in recognising 'Respect for private and family life' (Article 7) and protection of personal data (Article 8) as distinct rights. When considering patient information, it is important to recognise there are two distinct spheres, one of information privacy and one of data protection. Whilst not granting any legal priority to consent, the Charter does single it out as particularly important in stating that personal data 'must be processed on the basis of the consent of person concerned or some other legitimate basis laid down by law.' (Article 8(2)) The jurisprudence of the European Court of Human Rights and the Court of Justice of the European Union shows that

1 See Article 17 of the International Covenant on Civil and Political Rights: '17(1) No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. 17 (2) Everyone has the right to the protection of the law against such interference or attacks.'

2 *Guide on Article 8 of the European Convention on Human Rights*, Council of Europe, Update of 31 December 2020, para. 186, 186–190.

3 European Convention on Human Rights, Article 8: (1) 'Everyone has the right to respect for his private and family life, his home and his correspondence. (2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.'

despite substantial overlaps there are also important differences, in particular with regard to the scope of both rights and their limitations.[4]

Although often thought of as being about privacy protection, data protection is more about ensuring that when information flows, it does so legally, in an appropriate way, and with respect for defined rights of the data subject. The law and ethics of confidentiality relate more to the control that the patient has over information relating to them which they have shared in a particular (healthcare) context. This difference is important when considering the role and status of the protection provided by the requirement for implied consent in healthcare settings.

The European Standards on Confidentiality and Privacy in Healthcare (2006) ("European Standards") were developed by a group of experts from across Europe through the work of the EuroSOCAP Project (QRLT-2002-00771). The Standards were written to support the maintenance of confidentiality in healthcare and to manage tensions between confidentiality and information use and disclosure. Detailed consideration was given to the needs of vulnerable patients — particularly children and young people, older people, homeless people, people with mental health problems, prisoners, people with an intellectual disability, and people who lack decision-making capacity.[5]

The European Standards identified three key principles for the protection of the privacy of patients. These principles give a prime place to the role of consent:

> Individuals have a fundamental right to the privacy and confidentiality of their health information.
> Individuals have a right to control access to and disclosure of their own health information by giving, withholding or withdrawing consent.
> For any non-consensual disclosure of confidential information healthcare professionals must have regard to its necessity, proportionality and attendant risks.[6]

4 J. Kokott and C. Sobotta, 'The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR', *International Data Privacy Law* 3(4) (2013) 222–228; M. Tzanou, 'Data protection as a fundamental right next to privacy? "Reconstructing' a not so new right', *International Data Privacy Law* 3(2) (2013) 88–99.

5 EuroSOCAP Project, *European Standards on Confidentiality and Privacy in Healthcare* (Belfast: Queen's University Belfast, 2006), available online at https://fdocuments.net/document/european-standards-on-confidentiality-and-privacy-in-confidentiality-are-not.html (accessed 28 April 2022).

6 *Ibid.*, p. 5.

The weight to be given to these principles in application, varies depending on three distinct areas of use and disclosure of patient information:

(1) patient information might need to be shared with members of the multidisciplinary healthcare team for that patient's healthcare.
(2) the disclosure or use of confidential patient information may be important for purposes that are related to healthcare, but not to the care of the particular patient, for example, where patient information is used for audit or service provision or research to improve healthcare or treatment.
(3) confidential patient information held by a healthcare professional may have important uses outside the healthcare context, for example where a health care professional has information about the dangerousness of the patient to the public.[7]

The *European Standards* advise that: 'Express consent from the patient or their legal representative should wherever possible be obtained before any proposed secondary uses of patient personal information.'[8] However, many of the disclosures made in area 2 above are underpinned by statutory permissions or requirements or are subject to statutorily based review processes which provide independent scrutiny, but do not depend on patient consent.[9] Whilst consent is an option in this area, alternative legal routes usually exist. This is effectively broadly coherent with both the ECHR and the GDPR approach of multiple legal bases for lawful processing.

Required or permitted disclosures in area 3 above are also often underpinned by statute but are often justifiable by reliance on an overriding public interest. This also coheres with data protection approach which recognises public interests as bases of lawful processing (see GDPR Articles 6(1)(e) and 9(2)(g)). However, when it comes to area 1 above, that is where patient information is shared with members of the multidisciplinary healthcare team for that patient's healthcare, then the regulatory frameworks for use and disclosure diverge. Such disclosures rely, and must rely, on a protection of implied

7 *Ibid*., p. 4.
8 *Ibid*., p. 17.
9 Examples of the latter include the Health Service (Control of Patient Information) Regulations 2002 in England and Wales and the Health and Social Care (Control of Data Processing) Act (Northern Ireland) 2016 (which has yet to be implemented). Such legal processes which comply with the requirements of data protection law serve to provide procedural respect for patient confidentiality and address the challenges of situations where consent is not possible or practicable and anonymised data is not sufficient for the healthcare purpose. See M. Mostert, A.L. Bredenoord, M.C.I.H. Biesaart and J.J.M. van Delden, 'Big Data in medical research and EU data protection law: challenges to the consent or anonymisation approach', *European Journal of Human Genetics* 24 (2016) 956–960.

consent. This protection does not cohere with the framework of the GDPR as this requires consent to be explicit.

2 Consent and the General Data Protection Regulation

Within Regulation (EU) 2016/679 (General Data Protection Regulation) ('GDPR'), consent plays a role in that it is a potential condition for lawfulness of processing (Article 6(1)(a)) and for the processing of special categories of personal data (Article 9(2)(a)). There are other potential bases within the GDPR for lawful processing for treatment and general healthcare purposes other than consent, so whilst sufficient in data protection terms, it is not necessary. There are also particular challenges when seeking to rely on consent for health research purposes.[10]

Where the consent of the data subject is sought to be relied upon, the consent of the data subject must be 'explicit consent' and 'for one or more specified purposes'.

Recital 43 of the GDPR expresses reservations about reliance on consent which would apply to healthcare which is provided through a public authority:

(1) In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority, and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation.

(2) Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance.

There is thus a clear steer away from reliance on consent for the lawfulness of processing which in a European context will likely cover the majority of situations of processing for the purpose of individual patient healthcare.

10 M. Donnelly and M. McDonagh, 'Health research, consent and the GDPR exemption', *European Journal of Health Law* 26 (2019) 97–119.

Alternative bases for lawful processing are available. Under GDPR 'the basic concept of consent remains similar to that under the Directive 95/46/EC'.[11] However, Article 4(11) of GDPR provides an amended definition of consent:

> 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

This amended definition makes the requirements of 'explicitness' clearer and stronger.

The GDPR provides a range of possible alternative bases for lawful processing. Article 6 provides six bases for lawful personal data processing. Article 6 (1) (a) is where 'the data subject has given consent to the processing of his or her personal data for one or more specific purposes'. In relation to healthcare, Article 6 (1) (e) 'processing is necessary for the performance of a task carried out in the public interest' is clearly appropriate for data processing within healthcare.

With respect to 'special category' data, which includes health data, an additional condition must be met. GDPR Article 9(2) allows that the processing of such data can occur where:

> (a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes

This means that consent which is relied upon for the lawful data processing of health data must be explicit consent. In the practical delivery of patient healthcare, gaining and recording explicit consent for all data sharing in keeping with the data protection principles of specificity and necessity in GDPR

11 Article 29 Working Party on the Protection of Individuals with regard to the Processing of Personal Data, *Guidelines on consent under Regulation 2016/679* (wp259rev.01) Revised and adopted 10 April 2018 (Brussels: European Commission, 2018), available online at https://ec.europa.eu/newsroom/article29/items/623051 (accessed 28 April 2022), p. 4. The importance of the specific nature of consent in the GDPR was reaffirmed by the EDPB in the context of the coronavirus: European Data Protection Board, *Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak*, adopted 21 April 2020 (Brussels: European Data Protection Board, 2020), available online at https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032020-processing-data-concerning-health-purpose_en.

Article 5(1) is problematic. The need for healthcare to respond to the needs of patients on a case-by-case basis requires a flexibility of data sharing that is hard to force into a regime that operates within strict explicit consent which necessarily must be gained in advance of each occasion of data sharing. The GDPR conditions for lawful processing of special category data in healthcare which are better suited to the reality of healthcare delivery appear later in Article 9 (2) (h):

> processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3.

In consequence the GDPR requirements for 'lawful processing' of patient data (which includes its collecting, recording, storing, using or disclosing (Article 4(2)) are relatively easily met, particularly where there is a substantial public interest, or it is for some medical or social care purpose.

Given the strict requirements of explicit consent, it is generally recognised that consent is not an appropriate basis for lawful processing of personal data within healthcare. However, this applies only to data protection. The situation with respect to human rights or other legal and ethical informational privacy obligations may differ.

3 Consent and Informational Privacy

Consent plays a pivotal role in healthcare generally as the means by which patients exercise control over decisions made about their care and treatment. Part of the control patients exercise over their healthcare is control over the information they have shared for the purpose of their care and treatment. Patients have a right to control the access and disclosure of their own health information through the giving or withholding of consent. The place of consent in such health care decision-making remains unchanged by GDPR. The need for consent as a means of protecting a patient's private sphere remains even where the GDPR requirements for processing have been met.

The *European Standards* identified three key principles of informational privacy in healthcare:

(1) Individuals have a fundamental right to the privacy and confidentiality of their health information.
(2) Individuals have a right to control access to and disclosure of their own health information by giving, withholding or withdrawing consent.
(3) For any non-consensual disclosure of confidential information healthcare professionals must have regard to its necessity, proportionality, and attendant risks.[12]

There is a clear European consensus that from a privacy perspective consent remains central to giving patients control over the dissemination of their information. If the competent patient refuses to consent to disclosure, the information cannot be disclosed, unless, exceptionally, a justification other than consent exists.[13]

4 The Disclosure of Confidential Patient Information

There are generally three ways in which the disclosure of confidential information can be lawful: consent, a legal requirement or gateway, and an overriding public interest. In jurisdictions such as Ireland and the UK, in addition to human rights and data protection law, the sharing of information must also comply with the common law. In such jurisdictions the common law recognises that confidential information may lawfully be disclosed on the basis of an implied consent. In countries outside of Europe implied consent is again consider a valid option. For example, in both Australia[14] and in Canada,[15] 'consent' can mean express or implied consent.

When considering the disclosure of confidential healthcare information, the purpose of the proposed disclosure must also be considered. In particular whether the proposed disclosure is for the direct care of the person or persons in question or for some other purpose. First, patient information might need to be shared with members of the multidisciplinary healthcare team for that patient's healthcare needs, or it might be needed for auditing purposes, in

12 EuroSOCAP, *supra* note 5, p. 5.
13 *Ibid.*, p. 12.
14 Australian Medical Council, 'Consent and Informed Decision-making', in: *Good Medical Practice: Professionalism, Ethics and Law*, 4th edn. (Kingston, ACT: Australian Medical Council, 2016), https://www.amc.org.au/amc-good-medical-practice/ (accessed 28 April 2022).
15 Canadian Medical Association, *Principles for the protection of patient privacy* (Ottawa, ON: Canadian Medical Association, 2017), available online at https://policybase.cma.ca/viewer?file=%2Fmedia%2FPolicyPDF%2FPD18-02.pdf#page=1 (accessed 28 April 2022).

order to improve the patient's care. Second, in some situations, the disclosure or use of confidential patient information might be important for purposes that are related to healthcare, but not to the care of the particular patient, for example, where patient information is used for healthcare audit or research. Third, confidential patient information held by a healthcare professional may have important uses outside the healthcare context, for example where a health care professional has information about the dangerousness of the patient to the public. These three kinds of situation require separate considerations when deciding according to what criteria disclosure can be justified.[16]

5 Disclosure of Patient Identifiable Information for Direct Care

The justification for disclosure should normally be consent. As noted above the common law recognises that information may lawfully be disclosed on the basis of *implied* consent. When a patient presents to a doctor for treatment, it is generally implied that the information shared by the patient can be shared with others in order for treatment to be provided. 'A patient who consents to be referred to a specialist impliedly consents to medical information being provided to the specialist.'[17] While such disclosure is lawful in common law terms, it would not satisfy the requirements of lawful processing based on consent in terms of GDPR Articles 6 to 9. The UK Information Commissioner's Office recognises that:

> In the healthcare sector, patient data is held under a duty of confidence. Healthcare providers generally operate on the basis of implied consent to use patient data for the purposes of direct care, without breaching confidentiality.
>
> Implied consent for direct care is industry practice in that context. But this 'implied consent' in terms of duty of confidence is not the same as consent to process personal data in the context of a lawful basis under the UK GDPR.[18]

16 *Ibid.*

17 P. Stanley, *The Law of Confidentiality: A Restatement* (Oxford, Hart Publishing, 2008) pp. 49–52, at p. 51.

18 ICO GDPR, *ICO GDPR Guidance on "When is consent appropriate?"* (Wilmslow: ICO, 2022), available online at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/when-is-consent-appropriate/ (accessed 28 April 2022).

Processing personal health data without consent or when consent is being withheld can still be lawful processing. However, such lawfulness in data protection terms does not impact on the separate common law requirement for a defence to breach of confidence. If the breach is not required or permitted by law and nor is there a public interest justification, then consent is necessary for the lawful sharing or disclosure of personal health information for direct care. Unlike in the GDPR, the form of consent in the common law can be explicit or implicit.[19]

As with any other intervention in healthcare, patient consent occupies a pivotal role in legitimising the uses and disclosures of patient information. Patients and/or their legal representative must be informed of what information sharing is necessary for their healthcare. Provided they are informed in this way, explicit consent is not necessary, implied consent is sufficient for the ethical sharing of patient information for their healthcare.[20]

6 Disclosure of Patient Information for Healthcare Purposes not Directly Related to their Healthcare

As already noted, processing personal health data without consent or when consent is being withheld can still be lawful in terms of the GDPR if such processing meets one of the other necessary conditions for lawful processing. However, such lawfulness in data protection terms does not impact on the separate common law requirement for a defence to breach of confidence. Again if the breach is not required or permitted by law and nor is there a public interest justification, then consent is still necessary for the lawful sharing or disclosure of personal health information for other healthcare purposes. In particular a person's competent refusal should normally be respected.

However while the informed co-operation of a service user can provide a basis for inferring their consent to the use and disclosure of information required for their care, there is no behaviour which clearly implies consent to other uses and disclosures. Therefore when the proposed use or disclosure of identifiable information relates to healthcare but is not directly for the care of that service user, the common law requires that the express consent of that service user should normally be obtained.

19 Stanley, *supra* note 14, pp. 49–52.

20 'EuroSOCAP', *supra* note 5, p. 24.

7 Disclosure of Patient Identifiable Information for Purposes Outside the Healthcare Context

The justification for disclosure for purposes other than their healthcare should normally be consent. Where the patient is competent, only the patient can give consent to disclosure. However in some situations, healthcare professionals might be under a legal obligation to disclose information, or disclosure might be legally justified in the absence of consent.

In many European countries there are legal regulations governing the disclosure of confidential information that require the duty of confidentiality to be overridden, for example notification requirements with regard to certain communicable diseases. Where there is a legal obligation a healthcare professional is required to disclose the relevant information to the appropriate authorities to serve the public interest.

Disclosure of confidential information to third parties outside the health services may be justifiable in order to protect overriding interests of third parties or a legally protected public interest. However, every decision to disclose confidential patient information outside the healthcare services engages the patient's right to privacy and is in breach of the healthcare professional's obligation of confidentiality. The disclosure will only be justified in exceptional circumstances, that is, if the disclosure serves an interest that in the particular circumstances outweighs the patient's right to privacy. Potential outweighing interests could be the protection of the rights and freedoms of others, national security, public safety, the economic well-being of the country, the prevention of disorder or crime, or the protection of health or morals (as suggested by Article 8 (2) of the ECHR).

8 Implications

The foregoing considerations have implications for any proposed disclosure of confidential healthcare information:

(1) Disclosure for patient healthcare (direct care). Reliance on implied consent as a basic protection for sharing information for patient healthcare remains a key part of healthcare delivery in European Union and common law countries. It is important that it does not become eclipsed by an overemphasis on data protection law which risks obscuring the fundamental ethical and legal relationship of trust between a healthcare professional and their patient.

(2) Disclosure for healthcare purposes not related to the direct care. If the competent patient refuses to consent to disclosure, the information should not be disclosed, unless, exceptionally, a justification other than consent exists.

(3) Disclosure outside the healthcare context. Patient consent must be obtained unless there is a legal requirement to disclose or there is a clear overriding public interest. It is not sufficient that the proposed disclosure might serve the protection of such an overriding public interest; rather the test is one of strict necessity in the specific circumstances of each case.