

**European Standards on Confidentiality  
and Privacy in Healthcare among  
Vulnerable Patient Populations**

## CONTENTS

|       |  |    |
|-------|--|----|
| 1.    | Introduction   | 4  |
| 2.    | Ethical and Legal Foundations of the Standards   | 4  |
| 2.1   | Principles   | 4  |
| 2.2   | Ethical Basis of Privacy and Confidentiality in Healthcare   | 5  |
| 2.2.1 | Privacy and Confidentiality  | 5  |
| 2.2.2 | Justifications for Confidentiality   | 5  |
| 2.2.3 | Boundaries to Confidentiality  | 6  |
| 2.3   | The Legal Basis of Privacy and Confidentiality in Healthcare   | 7  |
| 2.3.1 | Privacy and Confidentiality  | 7  |
| 2.3.2 | Boundaries to Privacy and Confidentiality  | 9  |
| 2.3.3 | Country Specific Legislation and their Commonalities   | 10 |
| 2.4   | Vulnerability  | 11 |
| 2.5   | Balanced Decision Making   | 12 |
| 3.    | Standards  | 14 |
| 3.1   | Uses, Disclosures and Protections of Patient Information in providing Healthcare                                 |    |
| 3.1.1 | Keeping Patients Informed  | 14 |
| 3.1.2 | Consent to Uses and Disclosures of Patient Information   | 15 |
| 3.1.3 | The Impact of Forms of Vulnerability on the Uses and Disclosures of Patient Information for Healthcare Purposes. | 15 |
| 3.1.4 | Disclosure to a Patient's Carers   | 17 |
| 3.1.5 | Disclosure after a Patient's Death   | 18 |
| 3.1.6 | Multi-disciplinary and Inter-agency Working  | 19 |
| 3.1.7 | Access to a Patient's Healthcare Records   | 20 |
| 3.1.8 | Situations with Dual Obligations   | 21 |
| 3.1.9 | Security of Patient Information  | 22 |

|           |   |    |
|-----------|---|----|
| 3.2       | Uses, Disclosures and Protections of Patient Information for Healthcare Purposes not directly related to their Care | 24 |
| 3.2.1     | Administrative and Management Purposes  | 24 |
|           | (a) The Commissioning, Management and Administration of Health Services   | 24 |
|           | Consent   | 25 |
|           | Anonymisation   | 26 |
|           | (b) Clinical Audit  | 27 |
| 3.2.2     | The Use of Patient Information for Research   | 28 |
|           | Consent   | 28 |
|           | Anonymisation   | 31 |
|           | Research Databases  | 32 |
| 3.3       | Obligations and Justifications to Disclose Patient Identifiable Information   | 34 |
|           | (a) Obligations to disclose   | 34 |
|           | (b) Justifications for disclosure   | 35 |
| Appendix: | Summary of EuroSOCAP European Guidance on Confidentiality and Privacy in Healthcare                                 | 38 |

## **1. Introduction**

While each person's healthcare information is held under both ethical and legal obligations of confidentiality, there are a variety of situations where uses and disclosure of this personal information may occur for legitimate purposes.

For clinical practice purposes it is helpful to consider:

- the purpose of any planned use or disclosure
- the arrangements which must be satisfied to allow the use or disclosure.

In these Standards three categories of uses and disclosures are considered:

- (1) uses, disclosures and protections of patient information in order to provide healthcare.
- (2) uses, disclosures and protections of patient information for healthcare purposes not directly related to their care.
- (3) obligations and justifications for the disclosure of patient identifiable information used in the public interest.

Arrangements permitting specific uses and disclosure of patient information are considered for the following three situations:

- where the individual to whom the information relates has consented.
- where there is a duty to the public and disclosures are required by Law.
- where there is legal (Statute Law, Common Law) permission to disclose.

## **2. Ethical and Legal Foundations of the Standards**

### **2.1 Principles**

- 1 Individuals have a fundamental right to the privacy and confidentiality of their health information.
- 2 For any non-consensual disclosure of confidential information healthcare professionals must have particular regard to the necessity, proportionality and risks attendant upon the disclosure as well as to the complex set of diverse values in operation in any particular situation.

- 3 Individuals (or their carers or guardians) have a right to control the access and disclosure of their own health information or that of the minor for whom they have responsibility.
- 4 Individuals (or their carers or guardians) have a right to access in a timely manner their own health information or that of the minor for whom they have responsibility.

## **2.2 Ethical Basis of Privacy and Confidentiality in Healthcare**

### **2.2.1 Privacy and Confidentiality**

2.2.1.1 Privacy refers to the general interest in control of one's private sphere. The right to privacy, the right to respect for private life, is a well-established right, with a long tradition. This right guarantees the protection of the person against the intervention or interference of the public authorities in the private sphere. It embraces, but is not restricted to, the protection of personal information.

2.2.1.2 The right to protection of personal information is often referred to as the right to *confidentiality*. For doctors, the ethical requirement of confidentiality was first set out in the Hippocratic Oath which stated 'what I may see or hear in the course of treatment I will keep to myself holding such things shameful to be spoken about.' The World Medical Association affirmed the rule of confidentiality in the Declaration of Geneva (1948) and in the International Code of Medical Ethics (1949) which states: 'doctors shall preserve absolute secrecy on all he knows about his patient because of the confidence entrusted in him'.

### **2.2.2 Justifications for Confidentiality**

2.2.2.1 As the WMA rule indicates, and as is suggested by the word 'confidentiality', a major source of the requirement of confidentiality is the fact that the relationship between the doctor and the patient is, or should be, one of *confidence*. Whenever there is such a relationship, the doctor can be taken to have given an implicit *promise* not to disclose personal information, and the patient would and should *expect* that the information in question won't be shared with anyone else. A principle of respect for confidentiality can thus be justified by the fact that in a relationship of confidence there is a mutual understanding that personal information will not be divulged.

2.2.2.2 A different, albeit related, reason for not disclosing personal information is that the patient may not want it to be disclosed (whether or not there is a relationship of confidence). Just as the patient has a right to *self-determination*, or autonomy, in various other health care matters,

access to personal information is one of those things which patients largely ought to be able to decide for themselves whether or not to allow.

2.2.2.3 Third, it may also be argued that it is a matter of *dignity* not to share with others information which is personal. While a patient may not feel wronged by a disclosure which he or she has allowed, the patient may still be wronged by such a disclosure, if sharing the relevant information with others would violate his or her right to dignity. Thus, while the patient's consent to disclosure often would lift the confidentiality constraint, the fact that disclosure sometimes would infringe upon the dignity of the patient means that consent cannot be taken to automatically legitimize disclosure.

2.2.2.4 Each of these—the confidential nature of the relationship between doctor and patient, the patient's right to autonomy, and the patient's right to dignity—constitutes a *prima facie* reason for protection of personal information, and together they strengthen the case for non-disclosure. They can, in turn, be given further justification. For example, one reason for respecting confidences in healthcare is that doing so enables patients to disclose sensitive information that the doctor needs to carry out diagnosis and treatment. Without a confidentiality rule, patients might be much less willing to disclose such information, with negative effects for their health and medical practice. And the patient's right to self-determination in matters of information sharing could be justified on various grounds, including the view that the patient is the one who is in the best position to protect his own interests, or the view there is an intrinsic value in people deciding about, and taking responsibility for their own lives. With respect to ethical theory, some possible justifications are consequentialist, while others can be found in a deontological tradition. While their reasons differ, consequentialists and deontologists are typically united, however, in their commitment to a confidentiality requirement.

### **2.2.3. Boundaries to Confidentiality**

2.2.3.1 None of the foregoing ethical arguments leads to the conclusion that the clinician's duty of confidentiality is absolute. The confidentiality requirement exists within a wider social context in which clinicians have other obligations, moral and legal. These obligations may conflict with their duty of confidentiality. In particular, clinicians may have obligations to disclose confidential information, without consent, if serious and imminent dangers are present for third parties and where the clinician judges that the disclosure of that information is likely to reduce the danger. Clinicians also have other obligations towards the patient—of promoting his or her well-being, for instance—and it cannot be ruled out that those other obligations in some circumstances should outweigh the duty of confidentiality.

2.2.3.2 In assessing whether or not competing obligations outweigh the duty of confidentiality several things need to be considered. First, one would have to assess the nature, magnitude and probability of harm done to third parties by non-disclosure. What is at stake, for example: the health of third parties, their safety, or their psychological well-being? What is the worst case scenario, and how likely is it? Generally, in situations where both the probability and seriousness of harm done by non-disclosure are high, the moral obligation to disclose in order to prevent harm increases. Second, whether or not other duties trump the duty of confidentiality will also depend on the nature, magnitude and probability of harm done to patients by disclosure. For instance, might a disclosure, in the particular case at hand, ruin confidence, violate the patient's right to autonomy, and result in disrespect for his or her dignity? Or is perhaps only one of these values at risk? Generally, in situations where both the probability and seriousness of harm of disclosure are high, the moral obligation not to disclose personal information increases.

## ***2.3 The Legal Basis of Privacy and Confidentiality in Healthcare***

### **2.3.1 Privacy and Confidentiality**

2.3.1.1 Privacy and confidentiality are also legal concepts and the relationship between healthcare professionals and their patients carries with it legal obligations of confidence as well as ethical ones. For the Member States of the European Union, disclosure and use of personal information relating to a person's health are regulated by laws on privacy, confidentiality and data protection.

2.3.1.2 International Norms on Privacy. At an international level privacy is guaranteed by the following general instruments:

(1) Article 12 of the Universal Declaration of Human Rights (1948) states "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks".

(2) Council of Europe's Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) (ETS n<sup>o</sup> 005, 1950). The Convention is an international treaty which is binding on all those countries which have ratified it. The rights set forth in the Convention and case law of the Court are directly enforceable in domestic courts. Article 8 of the Convention states 'Everyone has the right to respect for his private and family life, his home and his correspondence'. The case law of the European Court of Human Rights (ECtHR) recalls that, although the essential object of Article 8 is to protect the individual

against arbitrary interference by the public authorities, there may in addition be positive obligations, and that in determining whether or not such a positive obligation exists, the Court will have regard to the “fair balance that has to be struck between the general interest of the community and the interests of the individual”. The ECtHR has acknowledged that the States enjoy a certain “discretion” as regards the need to restrict the guaranteed rights, but monitors the relevance and the proportionality of the reasons and the means of the interference undertaken by the national authorities. It leaves the States a wide margin of appreciation where there are diverse traditions or concepts of law in the national legal orders.

(3) Article 17 of the International Covenant on Civil and Political Rights (1966) states “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. Everyone has the right to the protection of the law against such interference or attacks”. Article 17 provides for a general protection, and as such does not define health related data, but these, as personal data elements of private life, are protected by the general provision.

2.3.1.3 European Norms on Confidentiality. Within the context of a confidential relationship (such as health care professional-patient), confidentiality concerns a small part of privacy, and as such is already protected by the general guarantee of privacy. Additional protection stems from the fact that confidentiality imposes an obligation on the person who obtained information in confidence not to disclose this information.

2.3.1.4 Article 8 of the ECHR. Confidentiality is necessary to maintain patients’ confidences in medicine and those responsible for their care, which is essential for the patient to seek medical advice and treatment and thus confidentiality participates in the promotion of public health. As the ECtHR has held, “Respecting the confidentiality of health data is a vital principle in the legal systems of all the Contracting Parties to the Convention. It is crucial not only to respect the sense of 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, thereby endangering their own health and, in the case of transmissible diseases, that of the community”. (Z v Finland 1997)

2.3.1.5 While decisions of the ECtHR show that the ECHR does not grant an absolute right to personal data confidentiality (see below), the protection granted to confidentiality is more extended in the Council of Europe

'Convention for the Protection of Individuals with regard to automatic processing of personal data' (No. 108). This Convention was the first international legally binding text in data confidentiality matters, and remains the only instrument of such a nature. It applies to all "automated personal data files and automatic processing of personal data in the public and private sectors" (article 3), as long as those data relate to "identified or identifiable individual" (article 2), whatever their nationality or place of residence. The notion of "data subject" in this Convention "expresses the idea that a person has a subjective right with regard to information about himself, even where this is gathered by others".

### **2.3.2 Boundaries to Privacy and Confidentiality**

2.3.2.1 Article 8 (2) of the ECHR states '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'.

2.3.2.2 At the level of the European Union, Directive 95/46 Article 8 deals with the processing of spe8ntedemo(oarieg)Tj0.00031 Tc 003423 Tw 12 0 0 12 184.79

### 2.3.3 Country Specific Legislation and their Commonalities

2.3.3.1 Throughout the EU, country specific human rights legislation incorporating the ECHR underpins all other legislation concerned with privacy. In addition public authorities are required to construe the legislation under which they operate in accordance with the European Convention on Human Rights. Country specific legislation giving effect to EC Directive 95/46 sets standards of information processing.

2.3.3.2 With the individual Member States of the European Union, laws on privacy and confidentiality are enshrined in statutes, civil/criminal codes or, in common law jurisdictions such as the UK, in the common law. In most countries of the European Union confidentiality and privacy are protected by statutory laws. For example, while the French constitution does not expressly protect the right to privacy the Constitutional Court has confirmed that privacy is a constitutional principle. Again in Germany the Federal Constitutional Court has argued that Articles 1 (1) and 2 (1) of the Basic Law grant every individual an inviolate sphere of private life. Unlike many European countries UK law does not recognise a general criminal offence of breach of professional secrecy. In the UK statutory duties of confidentiality are limited to special circumstances such as abortion or venereal diseases.

2.3.3.3 In those EU countries where confidentiality is not protected by statute, difficult judgements may arise in determining the threshold at which the justification for disclosure outweighs the obligation to maintain confidentiality.

2.3.3.4 In spite of the variety of provision, the overall direction is a strong protection of confidentiality in healthcare. The following summarises shared European principles on confidentiality:

(1) There is a *prima facie* obligation to maintain confidentiality when information has been imparted to a professional within a confidentiality relationship.

(2) This obligation can be discharged when the subject of the confidence affords appropriate informed consent to the disclosure of the information

(3) In providing a justification for the non-consensual disclosure of confidential information healthcare professionals should have particular regard to the following issues:

- (a) the necessity of any particular disclosure
- (b) the proportionality of any particular disclosure
- (c) the risks attendant upon any particular disclosure
- (d) the existence of identifiable risks of serious harm to identifiable third parties arising from non-disclosure

- (4) Where information is disclosed without the consent of the subject then the professional disclosing the information should be required to:
- (a) record what, if any, efforts have been made to obtain consent from that person;
  - (b) provide a written justification supporting the disclosure of the information without the consent of the subject
  - (c) inform the subject of the disclosure in advance that the disclosure will be made, unless informing the subject prevents the achievement of the justified aim of the disclosure.

## **2.4 Vulnerability**

2.4.1 The vulnerability of patients/clients is widely recognised across a range of patient groups and healthcare situations as a significant factor which warrants sustained ethical consideration.

There are certain individuals, who in general belong to specific well-recognised patient groups, who are vulnerable in a sense different to that in which it can be said that all human beings are vulnerable. It is important that in practice the perspective of those who are vulnerable in this specific sense should be at the centre of considerations about their vulnerability and its significance for decision making about the use and/or disclosure of their confidential information.

2.4.2 A vulnerable person is often less able to assert claims to rights that they possess, but can also have their rights violated as a result of a formal or informal label of 'vulnerable' being applied to them. It is important not to judge a *person* as being vulnerable as such in order to ensure that they do not thereby become stigmatized or subject to greater risk of discrimination. It is important to avoid making general judgements about a person. It is not a person as such who is vulnerable—to be 'vulnerable' in the particular sense means that something about a person or their life is vulnerable: (i) at a particular time; (ii) in some particular respect or respects (iii) to some particular harm or harms.

2.4.3 A particular person can move in and out of being vulnerable or the nature and extent of their particular vulnerability can change. It is important to recognise both that the vulnerability of a person changes over time and that it can have multiple and/or varying sources. The source of the vulnerability of a person can be from: their possession of a particular property (such as being ignorant of certain information, being ill or being particularly old or young); the result of them being in a certain place or environment (such as a prison, a refugee camp, or where they do not speak the language); or the result of occupying a certain position with respect to others (such as being a patient, being a member of a minority group, or being an asylum seeker).

2.4.4 It is important to consider that the full range of potential sources of a particular person's vulnerability in order to ensure that both the practical and ethical issues which arise from that vulnerability are properly addressed and fully considered. It is only when the concept of vulnerability is used of someone in a specific manner that its true significance for the confidentiality and privacy of that particular person can be determined.

2.4.5 Explicit attention to the vulnerability of people encourages better practical and ethical engagement with them, regardless of the ultimate ethical views or values of the health care professional or of the patient. Awareness of potential or actual vulnerability avoids unwarranted assumptions being made about the status of decision-making discussions where there are in reality significant power differentials. Such awareness helps to ensure that discussions about information use or disclosure between health care professionals and patients/clients take place on truly equitable terms.

## **2.5 *Balanced Decision Making***

2.5.1 In healthcare decision making, privacy and confidentiality, although important values in their own right, always have to be balanced against other values. This need for balanced decision making is reflected in the legal framework for privacy and confidentiality—for example, in the limitations of ECHR Art. 8 (2).

Balanced decision making about the use and disclosure of confidential patient information in day-to-day practice may require difficult judgements (para 2.3.3.3) and these judgements need to be supported by a clear legal and ethical regulatory framework. However, there are limits to the extent to which regulations alone can provide for balanced decision making. Balanced decisions, and the judgements on which these are based, also depend on good *process* in applying the general guidance defined by ethical and legal regulation in the particular concrete circumstances of individual cases.

2.5.2 The most important elements of 'good process' for balanced decision making about confidential information are:

- 1) Good decision making about the use and disclosure of confidential patient information requires an appropriate model of service delivery, specifically one that is both user-centred and multidisciplinary/multi-agency. Many vulnerable groups feel that professionals and policy makers consistently misjudge their real needs and interests and this makes it difficult for health care professionals to make ethically sound decisions about disclosure. Only when the vulnerable are empowered are their value perspectives given proper weight in making difficult balancing decisions about their confidential information. The relative

lack of decision making capacity of some people within vulnerable groups makes it essential that a variety of value perspectives is brought to play in coming to balanced decisions on individual cases. This balance of perspectives is provided in the case of clinical decision making by a well-functioning multi-disciplinary team.

2) Decision making about information use or disclosure with people from vulnerable groups should be closely geared to the particular and often highly diverse needs and values of the individuals concerned. This requires four key areas of professional skill: a) raised awareness of values and of diversity of values, b) improved knowledge of values and of diversity of values, c) reasoning skills for exploring differences of values, and d) communication skills in exploring values and in resolving differences of values.

3) Partnership between stakeholders with different value perspectives is particularly important. The guiding principle of partnership between those most directly involved in a given situation, as the basis of balanced decision making about uses and disclosure of confidential information, can be difficult to realise with vulnerable groups, although essential if their needs and interests are to be properly served.

Each of the elements of good process outlined above are likely to be relevant in supporting balanced decision making about uses and disclosures of confidential information with vulnerable groups.

### 3. Standards

#### 3.1 *Uses, Disclosures and Protections of Patient Information in providing Healthcare*

##### 3.1.1 Keeping Patients Informed

Providing useful and timely information to patients and carers is an essential element of an effective health service. Better communication with patients will enhance the partnership between patients and professionals and enhance the quality of their experience of care.

Modern health services frequently involve the sharing of information between healthcare professionals in order to provide optimal care and treatment. Patients may be unaware of what information is held about them, the kinds of purpose for which the information about them is used or the people with whom such information may need to be shared in order to provide their care and treatment. Patients must be made aware that information they give may be recorded, may be shared in order to provide them with care, and may be used to support clinical audit and other work to monitor the quality of care provided. Patients also need to be aware of the choices they have with respect to the uses and disclosure of the information they have shared in confidence with their doctor.

##### Policy Recommendation 1

Health Care Service providers must ensure that there is an active, effective and appropriate policy about informing patients or their representatives in each setting about the uses and disclosures of their information.

##### Guidance Point 1

Ensure that patients or their representatives are informed:

- of what kinds of information are being recorded and retained
- of what kinds of information sharing will usually occur between health professionals for evaluation, assessment, treatment, care
- of the choices available to them in respect of how their information may be used and disclosed
- about their rights to access and where relevant correct the information held about them within healthcare records
- the information required to be provided by national law implementing the Data Protection Directive

### **3.1.2 Consent to Uses and Disclosures of Patient Information**

As with any other intervention in healthcare, patient consent occupies a pivotal role in legitimising the uses and disclosures of patient information. Three conditions must be satisfied for consent to be effective. First it must be informed. A patient cannot be deemed to have consented to something of which they are ignorant. It is important that patients are made aware of the information sharing that must take place in order to provide them with appropriate care, including the requirements of for example clinical audit. Second the person giving consent must have some degree of choice. Thirdly there must be some indication that the patient has given consent. This may be expressed (explicit) or implied (implicit). Where patients have been informed of the uses and sharing of their information and the choices that they have, then expressed consent is not usually needed for the information sharing required to provide healthcare.

#### **Guidance Point 2**

Where patients or their representatives have been informed of the uses and sharing of the patient's information for their healthcare and of the choices that they have, then express consent is not usually necessary for information sharing needed to provide their healthcare.

### **3.1.3 The Impact of Forms of Vulnerability on the Uses and Disclosures of Patient Information for Healthcare Purposes**

3.1.3.1 While the provisions necessary for good practice in information sharing are relatively straightforward in many clinical situations, the presence of specific vulnerabilities, either because of the situation or a patient's condition, places significant challenges for healthcare providers to ensure that duties owed to patients are effectively discharged.

There are many overlapping sources of vulnerability, but a key one in the area of information sharing is patient vulnerability due to a lack of decision-making capacity. The consequences of this vulnerability for the effective protection of patient rights are not adequately addressed through the protections of the ECHR and mechanisms of the ECtHR.

#### Policy Recommendation 2

A common EU legal framework for the protection of the full range of rights and interests of all those who lack decision-making capacity should be developed as the context for all decisions about the use and disclosure of their confidential patient information. Such a framework should include provision for the independent review of such decisions.

3.1.3.2 Patients who lack capacity can also be harmed in their basic rights through a failure to identify such patients correctly. Effective measures must be in place at all levels of an institution to ensure that patients lacking decision-making capacity are correctly identified and that they receive the additional protection and empowerment that they need.

#### Policy Recommendation 3

Policies and procedures should be in place within health care institutions to ensure that patients who lack the capacity to make decisions about the use and disclosure of their confidential healthcare information are correctly identified.

3.1.3.3 Whilst a legal determination of a lack of decision-making capacity is a valid reason for additional protection, not all vulnerable patients in fact lack decision-making capacity. If a patient is determined to be technically competent to make decisions about the use and disclosure of their confidential information, there is then a need for a second evaluation as to their vulnerability in other respects. Although competent in the strict sense, many patients remain vulnerable to undue influence, exploitation and paternalistic treatment through an inability to assert their own interests and rights.

#### Policy Recommendation 4

A patient who has the capacity to make decisions about the use and disclosure of their healthcare information may nevertheless be vulnerable to undue influence and they should have the right of access to independent confidential support in the making of such decisions.

3.1.3.4 All patients, including the vulnerable, have a right not to be treated in a paternalistic manner and their exercise of their right to make decisions

about the use and disclosure of their confidential information should be facilitated to maintain it at the maximum level of which they are capable.

**Policy Recommendation 5**

Every patient should be involved in decisions about the use and disclosure of their confidential information to the greatest possible extent and all reasonable measures should be taken to ensure that participation in spite of a lack of capacity or presence of another factor of vulnerability.

3.1.3.5 'Vulnerability' must not be used in a vague and potentially discriminating manner, but in a precise and hence useful way. In order to ensure that the status of 'vulnerable' is not used in a vague and potentially discriminatory manner, any decision about the use or disclosure of confidential information made partly or wholly on the basis of a patient's vulnerability (however conceived) must be recorded along with the reasons for it.

**Guidance Point 3**

Whenever a competent patient is identified as vulnerable by a healthcare professional that identification, its specific nature and the justification for it, should with the patient's consent be recorded in any case notes.

**3.1.4 Disclosure to a Patient's Carers**

Families and other persons who are closely involved in the care of a patient have an understandable desire for information about a patient's healthcare problems and management. Such knowledge may benefit both the patient and the family, for example by better understanding of the nature of the patient's illness, or for promoting more appropriate responses to the patient and their needs. The fact that such information sharing may be beneficial does not lessen a patient's right to confidentiality. Particularly in situations of ongoing need for care and support, patients and their informal carers should be supported in reaching agreement on the sharing of information between them and how it should be handled.

**Policy Recommendation 6**

All formal carers should be bound by a contractual obligation with their employer to protect patient confidentiality.

**Guidance Point 4**

The potential benefits of information sharing with their informal carer should be discussed with the patient. Their wishes should be taken into consideration. Where a patient has the capacity to refuse disclosure to an informal carer and does refuse, their wish should be respected. Full consideration should be given to potential changes in the capacity of the patient.

**3.1.5 Disclosure after a Patient's Death**

The confidential nature of a patient's healthcare information and the obligation of the health care professional to respect that confidentiality are in no way changed by the death of that patient. However, just as in life, the right to privacy and the duty to maintain confidentiality are not absolute, but are subject to ethical and legal limitations of the kinds made clear in these Standards. (See 2.2.2.1-2.)

The death of a patient never in itself permits disclosure, but it does represent a changed situation for balanced decision-making. After the death of a patient it will be more common that the balanced ethical decision will be one favouring disclosure as the possible harm to which the confidant is subject as a result of disclosure is considerably reduced. The death of the patient does not automatically favour disclosure and an ethical balance must still be struck by the health care professional. Disclosures after death remain subject to all the usual ethical considerations governing disclosure, such as whether it is in the public interest or that any disclosure should be as minimal as possible. The health care professional must also be ready to justify their disclosure.

A patient can give or withhold consent to disclosure in advance of their death and such wishes must be respected as they would in other circumstances. In particular, where a patient has made an explicit request in advance of his or her death that their confidence be maintained in face of requests from family members or carers for disclosure, then that request should be respected.

**Guidance Point 5**

Where a patient has made an explicit request in advance of his or her death that their confidence be maintained in face of requests from family members or carers for disclosure, then that request should be respected.

### Guidance Point 6

Where a health care professional considers that disclosure after the death of a patient may be necessary, desirable or receives a request for disclosure and has no specific instructions, the professional should consider:

- the purpose of the disclosure and weigh it in the light of the usual considerations of harm and benefit insofar as they apply
- whether the disclosure may cause distress to or be of benefit to the patient's partner or family
- whether the information which is under consideration for disclosure includes information about others which is confidential
- whether the interests of a living person are judged to outweigh those of the deceased
- whether the information can be provided without identifying the patient.

Where a decision to disclose is made, the health care professional sanctioning the release of information should be clear about the grounds on which this is made and on whether or not there are any legal requirements.

### 3.1.6 Multi-disciplinary and Inter-agency Working

**Multidisciplinary work.** In many areas of healthcare doctors as part of their work will have professional contact with other professionals and other agencies delivering aspects of care. Other professional organisations and agencies may have different criteria and thresholds for the disclosure of confidential information, for example in relation to public safety.

### Policy Recommendation 7

Service providers must establish and ensure the adoption of publicly accessible protocols embodying these European Standards for information sharing within teams and beyond teams.

### Guidance Point 7

The healthcare team may include temporary members for particular functions and the team must not share information with temporary members unless they are under the same obligation of confidentiality.

Multidisciplinary teams should agree strategies for any disclosure of confidential information beyond the team.

Health care professionals are obliged to ascertain the thresholds for the disclosure of confidential information that other professional organisations and agencies may have.

**Interagency Work.** It is common practice in many areas of healthcare provision to involve outside agencies in the provision of services for patients. This inevitably involves discussions about patients at various points in their treatment. Issues concerning the sharing of information may arise in the context of verbal or written reports, or attendance at case conferences.

#### Policy Recommendation 8

Organisations providing healthcare should have publicly accessible protocols embodying these European Standards for the sharing of patient information between the organisation and outside agencies.

#### Guidance Point 8

Where it is planned to involve staff from other agencies this must first be discussed with the patient or their representative.

Where other agencies request information about patients, health care professionals should first seek the consent of the patient or their representative about such sharing including the content of information to be disclosed.

Where a competent patient refuses involvement of other agencies their refusal should be respected.

Where the representative of an incompetent patient refuses involvement of other agencies their refusal should be respected unless there are overriding considerations of the patient's best interests or of the public interest.

### 3.1.7 Access to a Patient's Healthcare Records

**Patient requests for access.** Patients have a right, both moral and legal, (EC Directive 95/46) to know what information a healthcare organisation holds in relation to them.

#### Policy Recommendation 9

Policies on a patient or their representative's access to healthcare records should be compliant with the provisions of country specific laws enacting the Data Protection Directive and other relevant laws.

#### Guidance Point 9

Health care professionals must respect patients' or their representatives' requests for access to their healthcare information.

### 3.1.8 Situations with Dual Obligations

Doctors may work in situations where they may have dual obligations. This includes work in prisons and for court liaison schemes where there are duties to both the patient and to the authority. Such dual obligations may cause conflict with regard to the confidentiality of patient information. For example a prisoner or defendant may have consulted a doctor on a previous occasion and divulged information that they do not wish an outside agency to know.

#### Policy Recommendation 10

The importance of avoiding placing healthcare professionals in situations where they have dual responsibilities with respect to the same patient should be given full weight in decisions about institutional structure and staffing.

#### Guidance Point 10

Health care professionals should avoid situations with dual responsibilities with respect to the same patient wherever possible.

Where a health care professional has dual responsibilities it is important that they explain at the start of any consultation or assessment on whose behalf they are seeing the patient and the purpose of the consultation or assessment. It should also be made clear to the patient or their representative that the information given will not be treated as confidential.

### **3.1.9 The Security of Patient Information**

3.1.9.1 The security of patient identifiable information, for example their healthcare records, is an essential aspect of confidentiality and information protection. The quality and integrity of patient information, information protection and the controls required to ensure that patient information sharing is secure, confidential and responsive to patient preferences are inextricably linked. Beyond the requirements of individual information initiatives a coherent framework for information governance is required. Within such a framework the two principal means of enhancing the security of clinical information are restriction of access and anonymisation of records.

#### **Policy Recommendation 11**

Access controls. Healthcare organisations must have in place systems and processes that will confine the use and disclosure of confidential patient information to those activities which are directly concerned with patient healthcare. Healthcare organizations must ensure adequate access controls and authentication procedures to prevent unauthorized access to patient identifiable information. All healthcare providers should have agreed protocols to protect patient information, including patient identification, with other healthcare organizations and with non-health organizations.

3.1.9.2 Anonymisation. Encryption is one method for anonymising electronically held information. It is the process by which data are converted into a sequence of alternative characters, by applying a set of rules (or key) that both generates the encrypted material and is capable of recreating the original information.

A complementary method for anonymising patient information is the use of separate databases in which clinical information is separated from patient-identifier information. The second database retains the non-identifiable patient information, which may be used for a range of purposes.

Aggregation is, ultimately, the one certain method of fully anonymising patient information.

Policy Recommendation 12

Anonymisation. Wherever possible, person-based information should be maintained in a non-identifiable form and, for the large healthcare databases, reconciliation of such information with patient identifiers should be restricted to appropriate circumstances and designated individuals.

3.1.9.3 While there are obligations on health service providers to ensure appropriate confidentiality and security arrangements, there are also obligations on all staff to keep information confidential. Given the nature of the doctor-patient relationship and the fact that most patient information is provided to doctors there is an important clinical governance element to safeguarding confidentiality. That is the handling of information and the maintenance of confidentiality through appropriate security measures is an important aspect of the quality of patient care.

Policy Recommendation 13

Anonymisation. Wherever possible, person-based information should be maintained in a non-identifiable form and, for the large healthcare databases, reconciliation of such information with patient identifiers should be restricted to appropriate circumstances and designated individuals.

Policy Recommendation 14

Training in security policies and protocols should form part of both induction training and in service training for all staff who may have access to patient identifiable information. Staff must be made aware of their obligations for maintaining confidentiality and security. Local guidance should include information on penalties for unauthorised access and breach of confidentiality.

Policy Recommendation 15

All staff who have access to patient identifiable information in the course of their work should have a contractual obligation to maintain confidentiality as part of their contract of employment.

Guidance Point 11

Given the clinical responsibility to maintain confidentiality, doctors should assure themselves that appropriate policies and protocols are in place and operational in their hospitals/units and among commissioners of services for the security of patient information.

### **3.2 *Uses, Disclosures and Protections of Patient Information for Healthcare Purposes not directly related to their Care***

#### **3.2.1 Administrative and Management Purposes**

##### **(a) The Commissioning, Management and Administration of Health Services**

3.2.1.1 Patient information is increasingly required for evidence based practice and a rational approach to service planning, management and commissioning. Secondary uses of confidential patient information are uses in healthcare which do not contribute directly to or support the healthcare that a patient receives.

The following is a non-exhaustive list of possible secondary uses:

- planning of services
- payment for services
- monitoring and protecting public health
- management of services
- contracting of services
- risk management
- investigating complaints
- auditing accounts and performance
- assuring and improving the quality of care and treatment, both local and national confidential inquiries into for example perioperative deaths, perinatal deaths
- teaching
- release of information for other Government departments outside healthcare
- research (dealt with separately)

3.2.1.2 The application of Information Technology (IT) has greatly facilitated the opportunities for exploiting the secondary uses of patient information. The establishment of large medical databases extracted and aggregated from individual clinical administrative data can be used to enhance healthcare evaluation and public health surveillance. They can be used for example to trace long term effects of drug actions, trajectories of particular diseases and outcomes of particular medical interventions.

The secondary uses of patient information raises particular concerns about confidentiality and security. One is the variability of practice on such issues as how much patient information is used, what procedures are followed to ensure confidentiality and where responsibilities lie. The introduction of IT to assist administrative and wider secondary uses raises additional concerns. Paper based medical records are typically locally located and maintained. Their unwieldy nature usually means they do not move much

beyond the primary location where patient care is delivered. However the extraction of patient information from such records onto other paper based systems or electronic information systems can lead to widespread dispersal of patient identifiable information.

One cannot assume that patients seeking healthcare are either aware of or content for their information to be used in these ways. Under the Data Protection Directive patients must be informed about such secondary uses and have a right to object to the use or sharing of confidential information that identifies them.

## **Consent**

3.2.1.3 Informed Implied Consent. All health service organisations must have policies for informing patients of the kinds of uses and disclosures of their information and the categories of people and organisations to which information may need to be passed in order for health services to do their task. Patients (or, in the case of minors, their parents or guardians) should be told how information will be used before they are asked to provide it and should be given an opportunity to discuss any aspects. It should be made clear to patients (or, in the case of minors, their parents or guardians) that they may object to specific secondary healthcare uses of identifiable information and that their objection will be respected. If patients (or their guardians) object to their information being used for a specific purpose this should be respected. The minimum necessary patient identifiable information should be used for each legitimate healthcare purpose.

Express Consent. Patient's express consent should be obtained in advance of all secondary disclosures to third party organisations (for example, voluntary organisations) or situations involving third parties (for example, teaching).

### **Policy Recommendation 16**

Informed implied consent may be appropriate for many secondary healthcare uses of patient information, that is, where information is not used for their direct care. Health providers must ensure that patients are informed of the secondary uses of their information and are aware of their choice on such issues. Where patients object to specific secondary uses their refusal must be respected. For all secondary healthcare uses of patient information involving third parties express informed consent must be obtained and appropriate procedures must be in place to ensure that such consent is obtained.

## **Anonymisation**

3.2.1.4 While the use of electronic media raises particular concerns (for example large centrally held databases), the same technology also offers viable solutions to such problems.

#### Policy Recommendation 17

Personal-based information should wherever possible be maintained in a non-identifiable form.

#### Policy Recommendation 18

There should be formal information sharing agreements with any other organisation that information is to be shared with.

#### Guidance Point 12



Given clinical responsibility to maintain confidentiality, health care professionals should assure themselves that appropriate policies and protocols are in place and operational in their hospitals/units and among commissioners of services for secondary healthcare uses of patient identifiable information.



Because anonymisation places data outside the reach of the data protection principles, auditors have a special interest in being able to claim that the data they are processing has been rendered anonymous in the terms of Recital 26. It is not unknown for auditors to make this claim for data that by no stretch of the imagination has been rendered anonymous. For example, auditors usually describe any data that does not actually have the subject's name attached as anonymous. In practice, designating data as 'anonymous' is a value judgment, and auditors should not use the term at all, but simply describe the form in which the data will be kept and processed, leaving it to the data subjects to decide what significance that has.

Auditors can best ensure that they act legally and ethically by informing patients of their intention to anonymise data and the effect that this will have, specifically the inability of patients to access their data and to know what is being done with it (and hence to object), whenever they intend to render it anonymous. This should not, however, be used as an excuse not to inform data subjects of the purposes of intended processing of data after rendering it anonymous. It should be used in cases where that data does not need to be kept in personal form and it is not known for what purposes it might be used.

**Policy Recommendation 19**

Whenever they intend to render data anonymous, auditors must inform patients of their intention to anonymise data and the precise effect that this will have—specifically the inability of patients to access their data and to know what is being done with it and hence to object. Data subjects must still be informed of the purposes of intended processing of data after it has been rendered anonymous. Anonymisation should be used in cases where that data does not need to be kept in personal form and it is not known for what purposes it might be used.

**(b) Clinical Audit**

3.2.1.5 Patient identifiable information will often be required for purposes which are aimed to support or assure the quality of patient care, for example clinical audit. Clinical Audit is an essential component of healthcare provision for which personal health information may need to be used. Patients in general (and the wider public) have a clear interest in the health services being subject to effective audit. As such they are part of the primary uses of patient information. Patients must be aware of such uses.

From an ethical perspective, a wide range of activities may be covered under the heading of audit by health service staff providing that care or treatment. Clinical audit is usually carried out wholly within the health service by staff directly involved in that patient's care. Implied consent is sufficient. However where information is going to be made available outside the health services, ethical review by a properly constituted body should be carried out in addition to the gaining of express consent.

**Policy Recommendation 20**

Use of patient information in processes of clinical audit involving staff not involved in the care of that patient require express consent for that use and should also be subject to ethical review.

**Guidance Point 13**

Health care professionals should assure themselves that appropriate policies and protocols are in place and are operational in their hospitals/units with respect to clinical audit.

**3.2.2 The Use of Patient Information for Research**

3.2.2.1 Research and the protection of confidentiality and privacy should not be seen as necessarily conflicting demands, but as mutually supportive ones. While there can be particular conflicts of interests between researchers, research subjects and those commissioning research, these must properly be understood as issues to be addressed rather than as inescapable features of the research process itself.

Research, because of its potential to improve the quality of patient's lives, is in important respects in the broad privacy interest of patients. Privacy is also in the research interest because research is facilitated by the willingness of patients and other research subjects to divulge sensitive information to researchers and to engage in research generally. However, if researchers attach too little importance to informational privacy, they endanger the needed trust of patients and of research subjects generally.

There is a need for a balanced approach to research governance that, besides protecting vulnerable people from exploitation, at the same time ensures that their rights to benefit from the results of research are not put at risk.

## Consent

3.2.2.2 Patient express consent should wherever possible be obtained in advance of any proposed uses of their personal information for research. Possible justifications for not obtaining consent for the use of patient information for research purposes are on the grounds of it being impracticable, inappropriate or impossible to do so considering the particular circumstances. It is important that these grounds for not obtaining consent are clearly distinguished.

- (a) When it is claimed that it is *impracticable* to obtain consent, it should be clear that the situation is very different when (i) dealing with data that has already been collected from now absent data patients than when (ii) dealing with patients who will be in front of the researchers when their data is obtained. It can never be impracticable to obtain consent in the latter case.
- (b) It might be *inappropriate* in the sense that the process of obtaining consent would itself involve a risk of further harm which the research is designed to minimize or prevent (for example, a public health emergency of some kind). Such cases of not obtaining consent would be *extremely* rare and could only arise where there is an immediate, pressing and clearly overriding public interest in doing so. In the absence of such a clearly defined interest, not gaining consent to the research use of confidential patient information cannot be justified.
- (c) It might be *impossible* in the sense that the confidential information was obtained for a particular research use, but that the potential for a

second use (and hence the ethical requirement for a second consent) has arisen which could not be foreseen at the time that the consent for the first research use was obtained. If the data has subsequently been unlinked from its initially consenting owners, then although they have a moral interest in its further use, gaining their further consent is impossible. Likewise, previously gathered information may have a research value beyond the death of the owner of that information when gaining further consent is impossible.

3.2.2.3 The best way forward in dealing with the kinds of situations of impracticality, inappropriateness and impossibility described above is to ensure that there is no abuse of these potential grounds for not obtaining consent for the research use of confidential patient information. Prevention of such abuse can best be achieved through the appropriate and widespread use of procedures to ensure ethical practice in advance of the research being conducted. In particular, independent data protection officers or Research Ethics Committees should be involved whenever judgments of impracticability, inappropriateness or impossibility are used as grounds for not upholding the full rights of data subjects. The Data Protection Directive permits the Supervisory Authority itself to be involved, but in the case of research this would be far too cumbersome and unworkable in countries with a large research activity.

It is also appropriate for such prior checking to occur whenever there is any exemption from the duty to provide information to patients about the processing of their data, simply because of the radical effect on their ability to protect their rights in cases of such exemption. Similar checking should also be provided whenever the right to object is removed.

#### Policy Recommendation 21

Independent data protection officers or Research Ethics Committees should be involved whenever judgments of impracticability, inappropriateness or impossibility of protecting rights to give or withhold consent to the research use of confidential patient information are involved. Such checking should occur whenever there is any exemption from the duty to provide information to patients about the processing of their data or whenever the right to object to such processing is removed.

Disclosure of identifiable information may be justified if the patient's informed consent has been obtained or exceptionally, the balancing exercise between the public interest in confidentiality and gains to the public interest by disclosure has been carried out (the opinion of a research ethics committee may assist in reaching a decision, although the opinion of the committee does not constitute legal authority for disclosure—responsibility is borne by the person disclosing information).

Guidance Point 14

Disclosure of identifiable information may be justified if:

Either:

(1) the patient's consent has been obtained

or:

(2) exceptionally, the balancing exercise between the public interest in confidentiality and gains to the public interest by disclosure has been carried out in advance by an independent authority and it has concluded that disclosure is justifiable.

3.2.2.4 It is important that the vulnerabilities of members of any group should not completely rule out their participation in research. The additional vulnerability of a potential research subject is properly the occasion for additional protection for them, not for their automatic exclusion from the individually and socially necessary undertaking of medical research.

In general the position of vulnerable research subjects with respect to their confidential medical information would be improved by a generalisation of the requirements of Directive 2001/20 EC on Clinical Trials (which only covers trials on medicinal products for human use) to other contexts of medical research, in the form of provision being required for a legal representative for adults with incapacities and children unable to make their own decisions.

Policy Recommendation 22

The requirements of Directive 20001/20/EC on the implementation of good clinical practice in the conduct of clinical trials should be generalized to other contexts of medical research, particularly in the form of provision being required for a legal representative for adults with incapacities and for children unable to make their own decisions.

## **Anonymisation**

3.2.2.5 Because anonymisation places data outside the reach of the data protection principles, researchers have a special interest in being able to claim that the data they are processing has been rendered anonymous in the terms of Recital 26. It is not unknown for researchers to make this claim for data that by no stretch of the imagination has been rendered anonymous. For example, researchers usually describe any data that does not actually have the subject's name attached as anonymous. In practice, designating data as "anonymous" is a value judgment, and researchers should not use the term at all, but simply describe the form in which the data will be kept and processed, leaving it to the RECs and research subjects to decide what significance that has.

3.2.2.6 Researchers can best ensure that they act legally and ethically by informing patients of their intention to anonymise data and the effect that this will have, specifically the ability of patients to access their data and to know what it is being used for (and hence to object to such uses). Such prior informing should not, however, be used as an excuse not to inform data subjects of the purposes of intended processing of data after rendering it anonymous. It should be used in cases where that data does not need to be kept in personal form and it is not known for what purposes it might be used.

#### Guidance Point 15

Every effort must be made to anonymize patient information before use in research.

#### Policy Recommendation 23

Whenever researchers intend to render data anonymous, they must inform patients of their intention to anonymise data and the precise effect that this will have— specifically the ability of patients to access their data and to know what it is being used for and hence to object to such uses. Data subjects must still be informed of the purposes of intended processing of data after it has been rendered anonymous. Anonymisation should be used in cases where that data does not need to be kept in personal form and it is not known for what purposes it might be used.

## Research Databases

3.2.2.7 Specific considerations apply where confidential patient information is to be stored in databases as a resource for research aimed at creating general knowledge and where such information is to be used as research data out of the context of those involved in the patient's care.

Traditional informed consent where participants are informed about particular research projects is only suitable for databases with clearly defined and restricted research uses that can be described prior to the collection of samples.

3.2.2.8 A form of communal consent is a valid way of ensuring that the creation of all databases occurs in a democratically legitimating manner. No new database should be established without preceding extensive public dialogue aiming to explain and assess its uses, purpose and public benefits. A database should not be established if there is a general dissent in the population to its creation. However, a general consent in the population to the creation of a database cannot replace the need for individual consent to be obtained from particular individuals for the inclusion of their confidential information in that database.

#### Policy Recommendation 24

No new database shall be established without preceding public dialogue aiming to explain and assess its uses, purpose and public benefits. A database should not be established if there is a general dissent in the population.

3.2.2.9 Consent to conditions for use. In those cases where it is impossible to foresee a potential research use of confidential information at the time of its collection, it is difficult to meet the requirements for informed consent without continuous re-contact which creates both a nuisance for participants and a serious hindrance to database research.

In such cases, the initial consent to the inclusion of participants' data could include consent to general conditions for use and should therefore ensure that potential participants are informed about details such as the following:

- which data will be placed into the database;
- how research on the data will be regulated;
- how privacy will be secured (non-technical);
- to what other data this data will be connected;
- who will have access to their information;
- that they will only be used for specified health care purposes;
- that the data will be used for the research of named diseases;

- that participants will be regularly informed about the research; practice and can opt out of the research if they choose.

Policy Recommendation 25

For those cases where it is impossible to foresee a potential research use of confidential information at the time of its collection, it is essential that the initial consent to the inclusion of participants' data include consent to general conditions for use of the database.

3.2.2.10 Ethical Review. All database research should be ethically reviewed. The Ethical Review Boards (or similar institutions) should judge what research is sufficiently important, as well as what precautions are sufficient to protect samples and information on sample providers, within the limits of national and international legal regulations. Ethical Review Boards should also decide when participants need to be contacted again (for example, when proposed research differs from the initial conditions for use).

Policy Recommendation 26

All research using databases of patient information should be ethically reviewed.

### **3.3 Obligations and Justifications to Disclose Patient Identifiable Information**

#### (a) Obligations to Disclose

3.3.1 In a number of European countries there are statutory regulations governing the disclosure of confidential information and either permitting or requiring the duty of confidentiality to be overridden. Where the obligation is a mandatory statutory obligation, a doctor is required to disclose the relevant information to the appropriate authorities. Failure to do so may lead to legal sanctions.

#### Policy Recommendation 27

Provider institutions must ensure that health care professionals are made aware of their country specific statutory requirements to disclose. This should, in particular, include the professional's duties with regard to disclosure requested by law enforcement agencies, professional regulatory bodies and the courts. Service users should also be provided with ready access to information about statutory regulations on disclosure of patient identifiable information.

#### Guidance Point 16

Where in the course of the health care professional-patient relationship an obligation to disclose is clearly becoming relevant to the healthcare professional, this should be discussed with the patient as early as possible unless such discussion would itself undermine the justification for the disclosure.

#### 3.3.2 Where a Court Orders the Disclosure of Information

In some European countries courts have powers to order the disclosure of documents prior to and during proceedings and to order the production of that material to an applicant and to their legal and professional advisers. Also during court proceedings a judge may order that medical records be disclosed, or that the doctor of a defendant answer questions about what the defendant has said or about the patient's medical history, condition etc.

### Policy Recommendation 28

Provider institutions must ensure that health care professional are made aware of the scope and limits of their duties to disclose information to courts; and to the legal consequences of disclosure or non-disclosure. Services users should also be provided with ready access to this information.

### Guidance Point 17

In those countries where a court has the power to order a health care professional to disclose confidential patient information, the health care professional must put before the court every argument that can properly be put against disclosure. Any disclosure must be limited to what is strictly relevant to the court proceedings.

### 3.3.3 Disclosure to Professional Regulatory Bodies

A statutory regulatory body may require patient records in order to investigate a health professional's fitness to practice and may have powers to require the disclosure. Where possible, the patient should be informed of this disclosure.

### Guidance Point 18

A health care professional working with a patient whose records are being requested for purposes of professional regulation has an obligation to raise any concerns over disclosure with the regulatory body. Where the regulatory body has the power to order disclosure and requires it, the request must be complied with and the patient should be informed.

### (b) Justifications to disclose

3.3.4 Disclosure of confidential information to third parties outside Health Services may be justifiable in the public interest on the basis of the harm averted by disclosure. However, as every decision to disclose confidential patient information outside the health care situation violates the patient's right to privacy and is in breach of the physician's obligation to confidentiality, it will only exceptionally be justified if the disclosure serves an interest that in the particular circumstances outweighs the patient's right to confidentiality. Such potential outweighing interests could be national security, public safety or the economic well-being of the country,

the prevention of disorder or crime, the protection of health or morals, or the protection of the rights and freedoms of others.

#### Policy Recommendation 28

Provider institutions must ensure that health care professionals are made aware of any country specific legal provisions or principles according to which the weighing of interests needs to be performed. Services users should also be provided with ready access to this information.

#### Guidance Point 19

In situations involving disclosure to third parties each case must be considered on its merits—the test being whether the release of information to protect one or more identified or identifiable members of the public, or the public at large, exceptionally prevails over the duty of confidence owed to the patient in the public interest. Decisions to disclose patient identifiable information outside the Health Services where no obligation to disclose information exists, are matters of judgment—judgment that may be finely balanced.

Factors that should be taken into consideration when reaching such a decision are, for example:

- (1) whether disclosure is really necessary to avert the harm; that is, that there is no possibility of averting the harm without disclosure;
- (2) the importance of the interest that is at risk without disclosure—for example, disclosure might be more easily justified where the life or physical integrity of a third party is at risk, but only in extremely rare circumstances can disclosure be justified where there is a serious risk to property;
- (3) the seriousness of the risk in the individual case—that is, disclosure might not necessarily be justified where there is a very remote risk to the life of another, but might be justified where there is a serious risk to the health of another;
- (4) the imminence of the risk of harm—that is disclosure might be justified where the risk requires immediate action, but not where there is no more than a possibility that at some future point in time the patient might cause a risk to others;
- (5) the likelihood that disclosure can avert the risk, which requires that the health care professional is satisfied that the harm to the other person or to society can be averted by disclosure.

Whether a breach of confidence is justifiable in the public interest will depend to some extent on the scope of disclosure. Therefore when considering whether to disclose, the health care professional should also consider the extent of the information to disclose and to whom it is appropriate and necessary to disclose such information.

In all instances where judgment is involved, clinicians are urged to discuss the case in an anonymised manner with colleagues and, if necessary, to seek legal or other specialist advice, including ones professional defence organisation or regulatory body.

Most of the situations where decisions to disclose are reached require good communication with and support for patients whose confidentiality is to be breached.

Once a decision has been reached that it is appropriate to disclose such information the usual procedure would be as follows. The exception to this normal procedure is where informing the subject of the disclosure in advance that the disclosure will be made would prevent the achievement of the justified aim of the disclosure.

- (1) an explanation of the reasons for sharing information should be given to the patient;
- (2) the clinician should encourage the patient to inform the relevant authority (for example, police or social services). If the patient agrees, the clinician will require confirmation from the authority that such disclosure has been made;
- (3) if the patient refuses to act as in the paragraph above, the clinician should then tell the patient that he/she intends disclosing the information to the relevant authority or person. He/she should then inform the authority, disclosing only relevant information and make available to the patient the information that he/she has released;
- (4) clinicians who decide to disclose confidential information (with or without prior informing of the patient) should be prepared to explain and justify their decision to the authority if called upon to do so. Clinicians should record in the healthcare record details of all conversations, meetings and appointments involved in the decision to disclose or not to disclose such information.

## **Summary of EuroSOCAP European Guidance on Confidentiality and Privacy in Healthcare**

1. Ensure that patients or their representatives are informed:
  - of what kinds of information are being recorded and retained
  - of what kinds of information sharing will usually occur between health professionals for evaluation, assessment, treatment, care
  - of the choices available to them in respect of how their information may be used and disclosed
  - about their rights to access and where relevant correct the information held about them within healthcare records
  - the information required to be provided by national law implementing the Data Protection Directive
  
2. Where patients or their representatives have been informed of the uses and sharing of the patient's information for their healthcare and of the choices that they have, then express consent is not usually necessary for information sharing needed to provide their healthcare.
  
3. Whenever a competent patient is identified as vulnerable by a healthcare professional that identification, its specific nature and the justification for it, should with the patient's consent be recorded in any case notes.
  
4. The potential benefits of information sharing with their informal carer should be discussed with the patient. Their wishes should be taken into consideration. Where a patient has the capacity to refuse disclosure to an informal carer and does refuse, their wish should be respected. Full consideration should be given to potential changes in the capacity of the patient.
  
5. Where a patient has made an explicit request in advance of his or her death that their confidence be maintained in face of requests from family members or carers for disclosure, then that request should be respected.
  
6. Where a health care professional considers that disclosure after the death of a patient may be necessary, desirable or receives a request for disclosure and has no specific instructions, the professional should consider:
  - the purpose of the disclosure and weigh it in the light of the usual considerations of harm and benefit insofar as they apply

- whether the disclosure may cause distress to or be of benefit to the patient's partner or family
- whether the information which is under consideration for disclosure includes information about others which is confidential
- whether the interests of a living person are judged to outweigh those of the deceased
- whether the information can be provided without identifying the patient.

Where a decision to disclose is made, the health care professional sanctioning the release of information should be clear about the grounds on which this is made and on whether or not there are any legal requirements.

7. The healthcare team may include temporary members for particular functions and the team must not share information with temporary members unless they are under the same obligation of confidentiality.

Multidisciplinary teams should agree strategies for any disclosure of confidential information beyond the team.

Health care professionals are obliged to ascertain the thresholds for the disclosure of confidential information that other professional organisations and agencies may have.

8. Where it is planned to involve staff from other agencies this must first be discussed with the patient or their representative.

Where other agencies request information about patients, health care professionals should first seek the consent of the patient or their representative about such sharing including the content of information to be disclosed.

Where a competent patient refuses involvement of other agencies their refusal should be respected.

Where the representative of an incompetent patient refuses involvement of other agencies their refusal should be respected unless there are overriding considerations of the patient's best interests or of the public interest.

9. Health care professionals must respect patients' or their representatives' requests for access to their healthcare information.

10. Health care professionals should avoid situations with dual responsibilities with respect to the same patient wherever possible.

Where a health care professional has dual responsibilities it is important that they explain at the start of any consultation or assessment on whose behalf they are seeing the patient and the purpose of the consultation or assessment. It should also be made clear to the patient or their representative that the information given will not be treated as confidential.

11. Given the clinical responsibility to maintain confidentiality, doctors should assure themselves that appropriate policies and protocols are in place and operational in their hospitals/units and among commissioners of services for the security of patient information.

12. Given clinical responsibility to maintain confidentiality, health care professionals should assure themselves that appropriate policies and protocols are in place and operational in their hospitals/units and among commissioners of services for secondary healthcare uses of patient identifiable information.

13. Health care professionals should assure themselves that appropriate policies and protocols are in place and are operational in their hospitals/units with respect to clinical audit.

14. Disclosure of identifiable information may be justified if:  
Either: (1) the patient's consent has been obtained  
or: (2) exceptionally, the balancing exercise between the public interest in confidentiality and gains to the public interest by disclosure has been carried out in advance by an independent authority and it has concluded that disclosure is justifiable.

15. Every effort must be made to anonymize patient information before use in research.

16. Where in the course of the health care professional-patient relationship an obligation to disclose is clearly becoming relevant to the healthcare professional, this should be discussed with the patient as early as possible unless such discussion would itself undermine the justification for the disclosure.

17. In those countries where a court has the power to order a health care professional to disclose confidential patient information, the health care professional must put before the court every argument that can properly

be put against disclosure. Any disclosure must be limited to what is strictly relevant to the court proceedings.

18. A health care professional working with a patient whose records are being requested for purposes of professional regulation has an obligation to raise any concerns over disclosure with the regulatory body. Where the regulatory body has the power to order disclosure and requires it, the request must be complied with and the patient should be informed.

19. In situations involving disclosure to third parties each case must be considered on its merits—the test being whether the release of information to protect one or more identified or identifiable members of the public, or the public at large, exceptionally prevails over the duty of confidence owed to the patient in the public interest. Decisions to disclose patient identifiable information outside the Health Services where no obligation to disclose information exists, are matters of judgment—judgment that may be finely balanced.

Factors that should be taken into consideration when reaching such a decision are, for example:

- (1) whether disclosure is really necessary to avert the harm; that is, that there is no possibility of averting the harm without disclosure;
- (2) the importance of the interest that is at risk without disclosure—for example, disclosure might be more easily justified where the life or physical integrity of a third party is at risk, but only in extremely rare circumstances can disclosure be justified where there is a serious risk to property;
- (3) the seriousness of the risk in the individual case—that is, disclosure might not necessarily be justified where there is a very remote risk to the life of another, but might be justified where there is a serious risk to the health of another;
- (4) the imminence of the risk of harm—that is disclosure might be justified where the risk requires immediate action, but not where there is no more than a possibility that at some future point in time the patient might cause a risk to others;
- (5) the likelihood that disclosure can avert the risk, which requires that the health care professional is satisfied that the harm to the other person or to society can be averted by disclosure.

Whether a breach of confidence is justifiable in the public interest will depend to some extent on the scope of disclosure. Therefore when considering whether to disclose, the health care professional should also consider the extent of the information to disclose and to whom it is appropriate and necessary to disclose such information.

In all instances where judgment is involved, clinicians are urged to discuss the case in an anonymised manner with colleagues and, if necessary, to seek legal or other specialist advice, including ones professional defence organisation or regulatory body.

Most of the situations where decisions to disclose are reached require good communication with and support for patients whose confidentiality is to be breached.

Once a decision has been reached that it is appropriate to disclose such information the usual procedure would be as follows. The exception to this normal procedure is where informing the subject of the disclosure in advance that the disclosure will be made would prevent the achievement of the justified aim of the disclosure.

- (1) an explanation of the reasons for sharing information should be given to the patient;
- (2) the clinician should encourage the patient to inform the relevant authority (for example, police or social services). If the patient agrees, the clinician will require confirmation from the authority that such disclosure has been made;
- (3) if the patient refuses to act as in the paragraph above, the clinician should then tell the patient that he/she intends disclosing the information to the relevant authority or person. He/she should then inform the authority, disclosing only relevant information and make available to the patient the information that he/she has released;
- (4) clinicians who decide to disclose confidential information (with or without prior informing of the patient) should be prepared to explain and justify their decision to the authority if called upon to do so. Clinicians should record in the healthcare record details of all conversations, meetings and appointments involved in the decision to disclose or not to disclose such information.