ASSOCIATION EUROPÉENNE DES MÉDECINS DES HÔPITAUX
EUROPEAN ASSOCIATION OF SENIOR HOSPITAL PHYSICIANS
EUROPÄISCHE VEREINIGUNG DER LEITENDEN KRANKENHAUSÄRZTE
EUROPESE VERENIGING VAN STAFARTSEN
DEN EUROPÆISKE OVERLÆGEFORENING
ΕΥΡΩΠΑΪΚΟΣ ΣΥΛΛΟΓΟΣ ΝΟΣΟΚΟΜΕΙΑΚΩΝ ΙΑΤΡΩΝ ΔΙΕΥΘΥΝΤΩΝ
ASSOCIAZIONE EUROPEA DEI MEDICI OSPEDALIERI
DEN EUROPEISKE OVERLEGEFORENING
ASSOCIAÇAO EUROPEIA DOS MÉDICOS HOSPITALARES
ASOCIACIÓN EUROPEA DE MÉDICOS DE HOSPITALES

EUROPEISKA ÖVERLÄKARFÖRENINGEN
EVROPSKO ZDRŽENJE BOLNIŠNIČNIH ZDRAVINIKOV
EUROPSKA ASOCIACIA NEMOCNICNÝCH LEKAROV
EUROPSKA UDRUGA BOLNIČKIH LIJEČNIKA

Document :	**AEMH 06/018**
Title:	**European Standards on Confidentiality and Privacy in Healthcare**
Author :	**EUROSOCAP**
Purpose :	**Information**
Distribution :	**AEMH Member Delegations**
Date :	**22 March 2006**

European Standards on Confidentiality and Privacy in Healthcare

www.eurosocap.org 2006

Contents

Preface

These European Standards on Confidentiality and Privacy in Healthcare were developed through the work of the EuroSOCAP Project (QRLT-2002-00771). EuroSOCAP is a European Commission funded project (2003-2006) established to confront and address the challenges and tensions created within the healthcare sector between the information or knowledge-based society and the fundamental legal and ethical requirements of privacy and confidentiality of healthcare information.

The Standards apply to all healthcare professionals and to healthcare provider institutions and address the areas of healthcare confidentiality and informational privacy. They provide background on the ethical and legal foundations of the Standards, guidance on best ethical practice for healthcare professionals and recommendations to healthcare provider institutions.

These European Standards are primarily ethical standards. They also consider European legal obligations upon healthcare professionals and the general legal context within which professional decisions about the protection, use and disclosure of confidential information take place. The legal context of this ethical guidance includes shared legal principles and law enforceable within Europe (such as the EU Data Protection Directive and the European Convention on Human Rights). Such laws do not exhaust the obligations on healthcare professionals to respect and protect patient confidentiality and privacy. Healthcare professionals may also need to exercise professional judgment. These Standards provide ethical guidance to all healthcare professionals in the making of such judgments. Best ethical practice also requires a supportive context and the Standards contain recommendations to healthcare provider institutions on those measures necessary for the most effective realization of the Standards in practice.

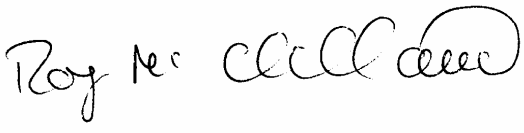
The Standards were written following detailed consideration of the needs of vulnerable patients—particularly children and young people, older people, migrants and mobile populations, prisoners, homeless people, people with mental health problems, people with an intellectual disability, and people who lack decision-making capacity. The explicit focus on the specific risks to the healthcare privacy and confidentiality of vulnerable patients has greatly informed the development of generic Standards to guide healthcare professionals, including practice involving vulnerable patients.

Copies of these Standards and the Guidance are available in various languages from the Project website at www.eurosocap.org. The website also provides: updates on items of interest in the area of healthcare confidentiality and privacy; a searchable database of links to relevant material; and a searchable database of experts and interested parties throughout Europe.

The Project team had 20 members—clinicians (with various specialisms), therapists, legal experts, and ethicists from 11 European states. Draft Standards were developed over a two year period by this team (with contributions from six invited experts). The draft Standards were then circulated widely for consultation during 2005 and were the subject of a Workshop attended by 80 experts from 26 European and neighbouring states. A broad range of responses were received through this consultation process, including perspectives from Patient Organizations, National Medical Associations, National Ministries of Health, National Data Protection Authorities, the European Commission, industry, universities, and relevant international organizations. Based on this consultation process, revised draft Standards were prepared and circulated for a further round of consultation. The Standards were finalized at a meeting of the EuroSOCAP Project Board in November 2005.

The work of the EuroSOCAP Project has been supported and informed by the work of others and the Project Board particularly wishes to thank the following:

Marie Brooks (Administrative Assistant to the EuroSOCAP Project);
the Confidentiality Advisory Group, Royal College of Psychiatrists, UK;
the PRIVIREAL project, (SIBLE, UK);
Vilhjálmur Árnason (University of Iceland & ELSAGEN Project);
Bernd Blobel (Health Telematics Project Group, Fraunhofer Institute, Erlangen);
Linus Broström (Department of Medical Ethics, Lund University);
Ruth Chadwick (CESAGEN & University of Lancaster);
Ethel Franz (Centro per la Scienza, la Società e la Cittadinanza, Rome);
Brandon Hamber (Independent Consultant);
Henk ten Have (Division of Ethics of Science and Technology, UNESCO);
Fanny Senez (European Forum for Good Clinical Practice, Brussels); and
the many stakeholders throughout Europe whose work contributed to the development of these Standards.



Roy McClelland,
Coordinator of the EuroSOCAP Project on behalf of the Project Team

Tom Berney	Deryck Beyleveld	Jesus Carbajosa
Francis Crawley	Beatrice Despland	Bill Fulford
Wolfgang Gaebel	Sefik Gorkey	Danielle Grondin
Marc Guerrier	Colin Harper	Goran Hermerén
Alastair Kent	Tony McGleenan	Sabine Michalowski
Emilio Mordini	Rosa Ordonez	Paul Thornton
Michael Weindling		

1. Introduction

All patients have the right to privacy and the reasonable expectation that the confidentiality of their personal information will be rigorously maintained by all healthcare professionals. Each patient's right to privacy and the professional's duty of confidentiality apply regardless of the form (for example, electronic, photographic, biological) in which the information is held or communicated. Not all healthcare professionals are bound by the same legal obligations of confidence, but all are under the same ethical obligations to maintain confidentiality. Particular care is needed on the part of healthcare professionals to ensure that the right to privacy of vulnerable patients is respected and that their duty of confidentiality toward them is fulfilled.

The aims of these European Standards are to:

- establish the ethical and legal framework and principles supporting the protection of confidentiality and informational privacy of people in healthcare;
- delineate the ethically necessary protections of confidential information and those circumstances where the use or disclosure of private or confidential information may be legitimate;
- provide Guidance on best ethical practice for healthcare professionals and policy Recommendations for provider institutions.

The ethical standards of healthcare professional confidentiality are not reducible to data protection standards, although they operate in conjunction with them. Further, confidentiality is an indispensable ethical complement to maintaining the security of information systems.

The high status of healthcare confidentiality can be found in several European Union (EU) laws. Directive 95/46/EC, the 'data protection directive', refers to certain data being 'processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy' (Article 8 (3)). Recital 9 of Directive 2001/20/EC on clinical trials refers to 'the rules of confidentiality'. However, the content of these 'confidentiality rules' in a European context has not been clarified. These Standards clarify these shared principles and rules within the rich diversity of the European community and in an international context.

While each patient's healthcare information is protected under both ethical and legal obligations of confidentiality, there are a variety of situations where the use and disclosure of personal information may occur for legitimate purposes. For practical purposes it is helpful to consider:

- the purpose of any planned use or disclosure of confidential healthcare information; and
- the criteria which must be satisfied to allow such use or disclosure.

In general, any use or disclosure of confidential healthcare information without consent, (for example, to the appropriate authorities at State level for health monitoring) should clearly serve one of the purposes specified in international human rights law as being a legitimate limitation on the right to privacy. Such disclosures must also meet the criteria of being proportionate to the legitimate aim of the disclosure, in accordance with (domestic) law, and taking place within the highest levels of data protection and data security.

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

- protections, uses, and disclosures of patient information for their healthcare (Section 3.2);
- protections, uses, and disclosures of patient information for healthcare purposes not directly related to their healthcare (Section 3.3); and
- obligations and justifications for the disclosure of patient identifiable information for purposes not related to their healthcare (Section 3.4).

2. Foundations of the Standards

2.1 Ethics, law, vulnerability

There are core principles of medical confidentiality and privacy which find expression in both ethical and legal norms. These are not simply rules, but rather guides for healthcare professionals in decision-making and aids for the promotion of ethical conduct in particular situations.

The protection of privacy and confidentiality is both an ethical obligation and a legal obligation. These are two different kinds of obligations, although normally what they require will be the same in a particular situation. They are not absolute obligations and must often be considered in the light of other obligations. Healthcare professionals have an ethical obligation to be aware of the nature and extent of their legal obligations. Health professional organisations should work to ensure that such legal obligations are in keeping with the ethical obligations of their profession. While healthcare professionals have an obligation to obey the law, doing so does not guarantee that they have behaved ethically.

Ethical standards may be different from the legal standards of a particular jurisdiction. Where the ethical standards require greater protection for patient confidentiality and privacy than the legal standards, then healthcare professionals should follow their ethical obligations and work to promote the protections required by ethics. Individual responsibility remains with the healthcare professional to ensure that they have acted ethically. Healthcare professionals should be aware of the importance of international human rights law and how these legal norms embody ethical principles which are both widely shared and deeply held across the world.

The needs of vulnerable patients are greater with respect to confidentiality—there is greater risk of their confidentiality being breached than is the case for other patients. Healthcare professionals have an ethical obligation to recognise vulnerable patients and to act appropriately. Achieving the same effective level of protection for vulnerable patients as for other patients may require greater attention.

2.2 Principles

The importance of maintaining confidentiality in the practice of healthcare has been recognised continuously over the two and a half millennia since the composition of the Hippocratic Oath. Medical confidentiality has been consistently upheld as a core value of European healthcare through profound cultural, technological, political, social and economic changes. It remains a core value to this day and in modern Europe finds expression in three key principles of healthcare confidentiality.

- 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 disclosure of confidential information healthcare professionals should have regard to its necessity, proportionality and attendant risks.

These principles find application in specific ways with different patient groups.

Guidance Point 1

Healthcare professionals should respect the following three key principles of healthcare confidentiality.

- 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.

2.3 The Ethical Basis of Privacy and Confidentiality

2.3.1 Privacy and confidentiality in ethics

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

For doctors, the ethical requirement of confidentiality was first set out in the Hippocratic Oath which states that '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).

2.3.2 Ethical justifications for confidentiality

As the rule of confidentiality in medical care indicates, and as is already suggested by the word 'confidentiality', a major source of the requirement of confidentiality is the fact that the relationship between the healthcare professional and the patient is, or should be, one of 'fidelity' or 'trust'. Within the relationship between the healthcare professional and the patient, there exists a tacit understanding on the part of the patient that confidential information will not be further used or disclosed without the awareness and consent of the patient. The patient has, thus, a reasonable expectation that information shared with the healthcare professional will not be further shared with anyone else.

A different, though related, reason for not using or disclosing personal information is that the patient may not want it to be used or disclosed. Just as the patient has a right to self-determination in various other healthcare matters, it is the patient's decision as to who should have access to personal healthcare information and how it should be used.

The confidential nature of the relationship between healthcare professional and patient and respect for the patient's autonomy constitute prima facie reasons for protection of personal information. Taken together they strengthen the case for the non-use or non-disclosure of private information about a patient. There are also other justifications. For example, one reason for respecting confidences in healthcare is that doing so enables patients to disclose sensitive information that the healthcare professional needs to carry out treatment. Without an assurance that confidentiality will be maintained, patients might be less willing to disclose information, resulting in negative effects for their health, for public health and for healthcare practice. The patient's right to self-determination in matters of information sharing could also be justified on other grounds. These include the view that the patient is in the best position to understand and therefore protect his or her own interests, and that there is an intrinsic value in people deciding about and taking responsibility for their own lives. In ethical theory, possible justifications can be in terms of the consequences of actions or rules, or can be in terms of duty. While their reasons differ, both of these approaches are united in their commitment to a confidentiality requirement.

2.3.3. Ethical boundaries to confidentiality

None of the ethical arguments stated above lead to the conclusion that the healthcare professional's duty of confidentiality is absolute. The confidentiality requirement exists within a wider social context in which healthcare professionals have other duties, which may conflict with their duty of confidentiality. In particular, healthcare professionals may have other ethical duties to disclose confidential information, without consent, if serious and imminent dangers are present for third parties and where the healthcare professional judges that the disclosure of that information is likely to reduce or eliminate

the danger. In assessing such risks and whether they outweigh the duty of confidentiality both the probability of the harm and its magnitude need to be considered. In situations where both the probability and seriousness of harm to a third party are high, the moral duty to disclose to prevent harm is greater.

2.4 The Legal Basis of Privacy and Confidentiality

2.4.1 Privacy and confidentiality in law

The relationship between healthcare professionals and their patients carries with it legal obligations of confidentiality as well as ethical ones. For the Member States of the European Union (EU), the disclosure and use of personal information about health are regulated by laws on privacy, confidentiality and data protection.

(1) International norms on privacy.
At an international level the protection of privacy, including healthcare privacy, is required by the following general instruments.

(1.1) Universal Declaration of Human Rights (1948). Article 12: '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'.

(1.2) International Covenant on Civil and Political Rights (1966). This is a treaty legally binding on all European Union states. Article 17: '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'.

(1.3) Universal Declaration on Bioethics and Human Rights (2005). Article 9: 'The privacy of the persons concerned and the confidentiality of their personal information should be respected. To the greatest extent possible, such information should not be used or disclosed for purposes other than those for which it was collected or consented to, consistent with international law, in particular international human rights law.'

(2) European norms on privacy and confidentiality.
Within the broader legal context, confidentiality in a professional relationship (such as healthcare professional and patient), is part of privacy, and already protected by the general right to privacy. Added protection stems from the fact that confidentiality imposes an obligation on the person who obtained information in confidence not to disclose this information.

(2.1) Charter of Fundamental Rights of the European Union (2000/C 364/01). Two articles of the Charter emphasize the importance of the protection of privacy: Article 7

states: 'Everyone has the right to respect for his or her private and family life, home and communications.' Article 8 states: '1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority.'

(2.2) Council of Europe's Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) (ETS nº 005, 1950 as amended). The ECHR is an international treaty which is binding on all those countries that have ratified it, which includes all EU Member States. Article 8 (1) 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) makes clear that the essential object of Article 8 is to protect the individual against arbitrary interference by the public authorities. There are in addition obligations on States to take positive steps to ensure that the right is respected, not merely to avoid measures which interfere with the right. In determining whether such a positive obligation exists, the Court will consider 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 State Parties enjoy some discretion in restricting the guaranteed rights, but monitors the relevance and the proportionality of the reasons and the means of the interference undertaken by 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.

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; MS v Sweden, 1997).

(2.3) Council of Europe 'Convention for the Protection of Individuals with regard to automatic processing of personal data' (No. 108) (1981). 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 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 on data confidentiality. 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 the data relates to an 'identified or identifiable individual' (Article 2), whatever their nationality or place of residence. According to the Explanatory Report to Convention No. 108, 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'.

(2.4) Council of Europe 'Convention for the Protection of Human Rights and Dignity of the Human Being with Regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine' (No. 164) (1997). The Convention on Human Rights and Biomedicine expands on many of the rights contained in the European Convention on Human Rights and elaborates how they apply in the field of medicine. Unlike the ECHR which applies to all EU Member States, the Convention on Human Rights and Biomedicine has not been signed or ratified by many States, including most of the larger States. In spite of it not applying directly to many EU States, it is nevertheless significant in that it has been drawn upon by the European Court of Human Rights in making judgments involving States who are not parties to this Convention. Article 10 of the Convention on Human Rights and Biomedicine states:

(1) Everyone has the right to respect for private life in relation to information about his or her health.
(2) Everyone is entitled to know any information collected about his or her health. However, the wishes of individuals not to be so informed shall be observed.
(3) In exceptional cases, restrictions may be placed by law on the exercise of the rights contained in paragraph 2 in the interests of the patient.

The recent 'Additional Protocol to the Convention on Human Rights and Biomedicine, concerning Biomedical Research' (No. 195) (2005) also emphasizes the importance of confidentiality. Article 25 (1) states that: 'Any information of a personal nature collected during biomedical research shall be considered as confidential and treated according to the rules relating to the protection of private life.'

2.4.2 Legal boundaries to privacy and confidentiality

Whilst patient privacy and confidentiality find legal protection at the national, the European and the international level, this protection is not absolute. The right to privacy of Article 8 (1) of the ECHR is limited by Article 8 (2) which 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'. Therefore to be compatible with the ECHR, any interference with the right to privacy must meet certain conditions. It must be 'in accordance with the law', which means that any interference must have some basis in national law, and the law must be precise enough so that people can reasonably understand its requirements and consequences. It must be 'necessary in a democratic society', which means that the interference must also both correspond to a 'pressing

social need' and be 'proportionate to the legitimate aim pursued'. Such 'legitimate aims' are exhaustively listed in Article 8(2).

Within the EU, Article 8 of Directive 95/46/EC 'on the protection of individuals with regard to the processing of personal data and on the free movement of such data' deals with the processing of special categories of data and in particular with data concerning health. Member States must prohibit the processing of those special categories of data, except in the situations (a) where the data subject has given his or her explicit consent; (b) where the processing is necessary to protect the vital interests of the data subject or of another person; and (c) where the data subject is physically or legally incapable of giving consent. Paragraphs 3 and 4 provide for other exceptions:

§3 '(…) where processing of the data is required for the purposes of preventative medicine, medical diagnosis, the provision of care or treatment or the management of healthcare services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.

§4 'Subject to the provision of suitable safeguards, Member States may, for reasons of substantial public interest, lay down exemptions (…) either by national law or by decision of the supervisory authority'.

Directive 95/46/EC is thus broadly in keeping with other international and European norms in this area.

2.4.3 Country specific legislation and their commonalities

In many Member States of the EU, country specific human rights legislation often incorporates the ECHR and thereby underpins all other legislation concerned with privacy. Country specific legislation giving effect to EC Directive 95/46/EC sets standards of information processing.

With the individual Member States, laws on privacy and confidentiality are enshrined in statutes, civil and criminal codes or, in jurisdictions such as the United Kingdom, in the common law. In most Member States 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 Constitution grant every individual an inviolate sphere of private life. Unlike in 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 disease.

Despite the variety of legal provisions, the overall direction across the Member States is a strong protection of confidentiality in healthcare. The following points summarise some shared European legal principles on confidentiality:

(a) there is a prima facie obligation to maintain confidentiality when information has been imparted to a professional within a confidentiality relationship;
(b) this obligation to maintain confidentiality can be discharged when the subject of the confidence affords appropriate consent to the disclosure of the information; and
(c) in providing a justification for the non-consensual disclosure of confidential information healthcare professionals should have particular regard to issues such as:
    (i) the necessity of any particular disclosure;
    (ii) the proportionality of any particular disclosure;
    (iii) the risks attendant upon any particular disclosure; and
    (iv) the existence of identifiable risks of serious harm to identifiable third parties arising from non-disclosure.

2.5 Vulnerability

2.5.1 The nature of vulnerability

Vulnerability refers to a circumstance in which a person finds himself or herself particularly susceptible to injury or harm. All patients in healthcare are vulnerable to misuses or abuses of their private information by healthcare professionals, healthcare providers, and by healthcare researchers. The circumstances of some persons (for example, children, the homeless or those with disabilities) can create particularly challenging situations for ethical and legal conduct.

The vulnerability of patients is a significant factor warranting ethical consideration and the perspective of those who are vulnerable should be at the centre of considerations for decision-making about the protection, use or disclosure of their confidential information.

A person in a vulnerable situation may be less able to assert claims to rights that they possess. They can also have their rights violated because of a formal or informal label of 'vulnerable' being applied to them. It is important not to judge a person as being vulnerable in such a way that they become stigmatised or subject to greater risk of discrimination. It is not a person who is vulnerable but rather some aspect of their circumstances that makes them vulnerable: that is, at a particular time; in a particular way; and vis-à-vis a particular harm or harms.

A person can move in and out of being vulnerable, and the nature and extent of their particular vulnerability can change and can have multiple and/or varying sources. The source of the vulnerability of a person can be a result of (a) their possession of a particular characteristic (such as being ignorant of certain information, being ill or being old or young); (b) their being in a certain place or environment (such as a prison, a refugee centre, or a place where they do not speak the language); (c) occupying a certain position with respect to others (such as being a member of a minority group, or being an asylum seeker); or (d) several or all of the above.

It is important to consider the full range of potential sources of a patient's vulnerability to ensure that both the ethical and practical issues which arise from that vulnerability are fully considered and properly addressed. It is only when the concept of vulnerability is used of someone in a specific manner that its true significance for the privacy and confidentiality of that particular person can be determined. For example, adolescents may be vulnerable because of assumptions made simply on the grounds of chronological age about their ability to make competent decisions. In many prison situations, the right of a prisoner to privacy, including the right to privacy of health information, is compromised. A refugee may be faced with disclosure requirements as part of a pre-departure health assessment. Someone with impaired capacity, for example a person with an intellectual disability or dementia, may be unable to make decisions about the use or disclosure of their health information. A person with severe and enduring mental illness may face expectations to disclose personal information with regard to risk management. Some people may have multiple sources of vulnerability—for example a migrant child with an intellectual disability within the criminal justice system—and such a person's vulnerability must be understood in its complexity, especially where one vulnerability can obscure the existence of others.

Explicit attention to the vulnerability of a person encourages better practical and ethical engagement with them, regardless of the ethical views or values of the healthcare professional or of the patient. Awareness of vulnerability avoids unwarranted assumptions being made about the status of decision-making processes where there are significant power differentials. Such awareness helps to ensure that discussions about information use or disclosure between healthcare professionals and a patient (or their legal representative*, such as a parent or guardian) can take place on fair terms.

2.5.2 The impact of vulnerability on the protection, use and disclosure of patient information

Article 8 of the Universal Declaration on Bioethics and Human Rights (2005), states: 'In applying and advancing scientific knowledge, medical practice and associated technologies, human vulnerability should be taken into account. Individuals and groups of special vulnerability should be protected and the personal integrity of such individuals respected.' While the provisions necessary for good practice in information sharing are fairly straightforward in many clinical situations, the presence of specific vulnerabilities, either because of the patient's condition or their situation, poses significant challenges for healthcare providers and healthcare professionals.

There are many overlapping sources of vulnerability, but a key one in information sharing is patient vulnerability because of a lack of decision-making capacity. (See 3.1.1

* Throughout these Standards, 'legal representative' refers to a person provided for by law to represent the interests of, and/or take decisions on behalf of, a person who does not have the capacity to consent.

and 3.1.2.) The consequences of this vulnerability for the effective protection of patient rights are not adequately addressed through the protections of the ECHR.

Recommendation 1

A clear institutional framework to protect 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 protection, use and disclosure of their confidential patient information. Such a framework should include provision for the independent review of such decisions and be in accordance with the relevant laws of the jurisdiction.

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 added protection and empowerment they need.

Recommendation 2

Policies and procedures should be in place within healthcare institutions to ensure that patients who may lack the capacity to decide about the protection, use and disclosure of their confidential healthcare information are correctly identified.

While a legal determination of a lack of decision-making capacity with respect to the use and disclosure of their information is a valid reason for added protection, not all vulnerable patients lack that capacity. Although legally competent to make decisions, many patients remain vulnerable to undue influence and/or exploitation through an inability to assert their own interests and rights.

Recommendation 3

A patient who has the capacity to decide about the protection, use and disclosure of their healthcare information may nevertheless be vulnerable to undue influence. Patients should have access to independent confidential support to make such decisions.

Guidance Point 2

Healthcare professionals should ensure that vulnerable people are given all necessary support to enable them to understand the complexities of confidentiality issues and to help them to express their wishes.

All patients, including the vulnerable, must be treated with respect. In particular, their exercise of their right to decide about the use and disclosure of their confidential information should be facilitated.

Recommendation 4

Patients should be involved to the greatest extent possible in decisions about the protection, use and disclosure of their confidential information. All reasonable measures should be taken to ensure maximum participation in spite of any vulnerability.

Views of a patient's 'vulnerability' may contain judgements by the healthcare professional about values which may not be shared by the patient and due care must be taken that 'vulnerability' is not being used in a vague and potentially discriminatory manner, but in a precise and useful way. Any decision about the use or disclosure of confidential information based partly or wholly on a patient's vulnerability and the possible harms to which it exposes them should, with their consent or that of their legal representative, be recorded in their case notes with the reasons for the decision.

Guidance Point 3

Whenever a patient is identified as vulnerable by a healthcare professional, that identification, its specific nature and the justification for it, should, with the consent of the patient or their legal representative, be recorded in their case notes.

2.6 Balanced Decision-making

Within the framework of fundamental rights of the patient, there is a need for balanced ethical decision-making about the protection, use and disclosure of confidential information. In healthcare decision-making, privacy and confidentiality, although important values in their own right, often have to be balanced against other values. The value placed on privacy and confidentiality can vary between patients and for the same patient in different contexts. Good decision-making will take full account of the values and fundamental beliefs of the patient concerned.

Balanced decision-making about the use and disclosure of confidential patient information in day-to-day practice may require difficult judgements and these judgements need to be supported by a clear framework of ethical and legal obligations. 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 individual cases.

The following are the most important aspects of the process for balanced decision-making about uses and disclosures of confidential information:

(a) Good decision-making about the use and disclosure of confidential patient information needs an appropriate model of service delivery, specifically one that is both

user-centred and multidisciplinary/inter-agency. Many vulnerable people feel that professionals and policymakers consistently misjudge their real needs and interests, making it difficult for healthcare professionals to make ethically sound decisions about disclosure. Only when the vulnerable are empowered are their perspectives on what is most valuable in their lives given proper weight in making difficult balancing decisions about their confidential information. The relative lack of decision-making capacity of some vulnerable people makes it essential that various perspectives on what is valuable are brought to play in coming to balanced decisions in particular situations. This balance of perspectives is provided in the case of clinical decision-making in part by a well-functioning multidisciplinary team. However, the healthcare team does not necessarily contain the value perspective of the patient, which underlines the importance of keeping patients (and where appropriate, their legal representative) informed about the possible uses and disclosures of their information and of their choices in this regard.

(b) Decision-making about information protection, use or disclosure with people from vulnerable groups should be closely focused on the particular and often diverse needs and values of the individuals concerned. This requires four key areas of professional skill: (i) awareness of values and of the diversity of values; (ii) knowledge of values and of the diversity of values; (iii) reasoning skills for exploring differences of values; and (iv) communication skills in exploring values and in resolving differences of values.

(c) Partnership between stakeholders with different value perspectives is important. The guiding principle of partnership between those most directly involved in a given situation is essential if their needs and interests are to be properly served—this may be difficult to realise with vulnerable groups.

3. Standards

3.1 Protection, Use and Disclosure of Patient Information—General Considerations

In principle, patient information is confidential and should not be disclosed without adequate justification. In many instances disclosure of confidential information, or its use, are desirable or necessary. 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 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 research. Third, it is possible that 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 situations to some extent require different considerations when deciding according to what criteria disclosure can be justified and are dealt with separately under

Sections 3.2, 3.3 and 3.4 below. Some considerations, however, are common to all situations and these are outlined below.

3.1.1 Patient consent

The justification for disclosure should normally be consent. Where the patient is competent, only the patient can give consent to disclosure.

Consent is a means by which the competent patient can exercise control over the dissemination of confidential patient information. Valid consent requires that the patient has been informed as to what information it is intended to disclose, and for which purposes disclosure is proposed. Consent also presupposes choice, which means that the patient who is asked to consent must have the possibility to refuse or withdraw such consent. (See 3.2.2)

If the competent patient refuses to consent to disclosure, the information cannot be disclosed, unless, exceptionally, a justification other than consent exists (see 3.4). The healthcare professional should discuss with the patient why he/she thinks that disclosure is in the patient's best interests. However, it can never be justified to disclose information in the best interests of the competent patient who refuses to consent to disclosure, as it is the competent patient, not the healthcare professional who decides what the competent patient's best interests are.

3.1.2 Circumstances where a patient is unable to consent

There are circumstances where a patient is unable to consent to the use or disclosure of their confidential information and in such circumstances, special considerations apply.

Incapacity. The precise definition of incapacity, how it is to be determined, and the status of any legal representative, who would have the right to give proxy consent to uses and disclosures on behalf of an incompetent patient, depend on country-specific law. The control a legal representative exercises over the patient's information is usually more limited than that exercised by the patient him/herself while competent, as legal representatives have to act in the patient's best interests. Where a healthcare professional thinks that disclosure would be in the best interests of a patient unable to consent, he/she should raise this with the patient's legal representative. If the consent of the legal representative is withheld, the healthcare professional might involve the court to settle the dispute.

Guidance Point 4

Where a healthcare professional thinks that disclosure would be in the best interests of a patient unable to consent, he/she should raise this with the patient's legal representative (including the parent/guardian of a minor). If the consent of the legal representative is

withheld, the healthcare professional should follow the current best practice of their country in resolving the dispute.

Emergency Situations. In emergency situations it may be impossible to keep a patient and/or their legal representative properly informed and to gain their consent. In such situations, uses or disclosures may be made, but only the minimum necessary information should be used or disclosed to deal with the emergency situation.

Guidance Point 5

In emergency situations, uses or disclosures of confidential patient information may be made, but only the minimum necessary information should be used or disclosed to deal with the emergency situation.

3.1.3 Disclosure to protect interests that override the patient's right to confidentiality

Exceptionally, it might be justified to disclose confidential patient information where disclosure is necessary to protect interests that override the patient's right to confidentiality. This is dealt with in more specific terms in 3.4.2, but as a general principle, it is important to remember that the interests of the competent patient cannot justify disclosure against the patient's wishes. Thus, where the patient is competent, disclosure without consent can only be justified if it is exceptionally necessary to protect the overriding rights of *others*, or there are overriding legally protected public interests. With regard to the incompetent patient, disclosure might also be justified to protect overriding interests of the incompetent patient, for example where disclosure is necessary to protect the incompetent patient from sexual abuse.

3.1.4 Disclosure after a patient's death

The confidential nature of a patient's healthcare information and the healthcare professional's obligation to respect that confidentiality are not changed by the death of that patient. However, just as in life, the right to privacy and the duty to maintain patient confidentiality after their death are not absolute, but are subject to ethical and legal limitations.

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 favour disclosure, as the possible harm to which the dead patient is subject is considerably reduced. The death of the patient does not automatically favour disclosure and an ethical balance must still be struck by the healthcare professional. Disclosures after death remain subject to the ethical considerations governing any disclosure, such as whether disclosure serves a legally protected public interest and that any disclosure should be as minimal as possible.

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

Guidance Point 6

The confidentiality of patient information must be maintained after the death of the patient.

Guidance Point 7

Where a competent patient has made an explicit request before his or her death that their confidence be maintained, then that request should be respected.

Guidance Point 8

Where a healthcare 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 from that patient, the professional should consider this as a situation of possible disclosure to third parties or disclosure for a legally protected public interest. (See Guidance Points 19-23.)

3.1.5 Patient access to their healthcare records

Patients have a right, both ethical and legal (EC Directive 95/46/EC on data protection), to know what information a healthcare professional holds in relation to them and disclosure of their healthcare records to the patient is thus always justified.

Guidance Point 9

Healthcare professionals must respect patients' requests for access to their healthcare information and comply with their legal obligations under Data Protection laws.

3.2 *Protection, Use and Disclosure of Patient Information for Their Healthcare*

3.2.1 Keeping patients informed

That patients must be kept informed about the possible uses and disclosures of their information is a binding legal obligation across the EU. Keeping patients fully informed is also essential for maintaining the relationship of confidentiality. Better communication

with patients (and/or their legal representative) will also improve the partnership between patients and professionals enhancing the quality and experience of their care.

Modern health services often involve sharing information between healthcare professionals to provide optimal care and treatment. Patients may be unaware of what information is held about them, the purposes for which the information is used or the people with whom such information may need to be shared to provide their care. Patients and/or their legal representative must be made aware that information given may be recorded and shared to provide the patient with care. It may also be used to support clinical audits and other work to monitor the quality of care provided. Patients and/or their legal representative, also need to be aware of the choices they have for the use and disclosure of the information shared in confidence with a healthcare professional.

It is an ethical and legal requirement that patients are both kept informed of all circumstances in which they can give or withhold consent to the use of their information and given information necessary for that consent.

Recommendation 5

Healthcare service providers must ensure there is an active, effective and appropriate policy about informing patients and/or their legal representative in each setting about the protections, uses and disclosures of their information.

Guidance Point 10

Healthcare professionals must ensure that patients and/or their legal representative are informed in a manner appropriate for the patient's communication needs:

- of what kinds of information are being recorded and retained;
- of the purposes for which the information is being recorded and retained;
- of what protections are in place to ensure non-disclosure of their information;
- of what kinds of information sharing will usually occur;
- of the choices available to them about how their information may be used and disclosed;
- about their rights to access and where necessary to correct the information held about them within healthcare records;
- the information required to be provided to them by national law implementing Directive 95/46/EC; and
- country specific legal provisions or principles governing disclosure.

3.2.2 Consent to the use and disclosure 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. 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.

Guidance Point 11

Patients, or where appropriate their legal representative, must be informed of what information sharing is necessary for the patient's individual 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.

3.2.3 Clinical audit

Patient identifiable information will often be required for purposes which aim to support or assure the quality of patient care, for example clinical audit. Processes of clinical audit are an essential part 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. Audits are part of the primary uses of patient information. Patients and/or their legal representative must be aware of such uses.

From an ethical perspective, a wide range of activities by health service staff providing that care or treatment may be covered under the heading of audit. Clinical audit which makes use of confidential patient information is usually carried out within the health service by staff directly involved in that patient's care. Implied consent is sufficient.

Provider institutions must ensure that patient express consent (or that of their legal representative) is obtained for processes of clinical audit by staff not involved in the care of that patient. Where it is proposed to make information available outside the health provider institution, the audit process should also be subject to ethical review.

Recommendation 6

Provider institutions must ensure that the express consent of the patient (or of their legal representative) is obtained for processes of clinical audit by staff not involved in the care of that patient. Where it is proposed to make information available outside the health provider institution, the audit process should also be subject to ethical review.

Guidance Point 12

Healthcare professionals should strive to ensure that institutional policies for clinical audit are compatible with the ethical requirement for confidentiality.

3.2.4 Disclosure to a patient's carers

All people employed by or working in organisations providing healthcare should be under an obligation of confidentiality.

Recommendation 7

All organisations providing healthcare should ensure that all people employed by or working in the organisation are under a legal obligation to protect patient confidentiality.

Families and other persons who are caring for a patient have an understandable desire or need for information about a patient's healthcare problems and management. Such knowledge may benefit both the patient and the carer by, for example, creating a better understanding of the patient's illness, or by promoting more appropriate responses to the patient and their needs. However, the fact that such information sharing may be beneficial does not diminish the duty of confidentiality owed to the patient by the healthcare professional. In situations of ongoing need for care and support, the potential benefits of information sharing with their informal carers should be discussed with the patient and/or their legal representative.

Guidance Point 13

The potential benefits of information sharing with their informal carer should be discussed with the patient and/or their legal representative. However, the fact that such information sharing may be beneficial does not diminish the duty of confidentiality owed to the patient by the healthcare professional.

3.2.5 Multidisciplinary and Inter-agency working

It is good practice that when a healthcare professional legitimately discloses information in a multidisciplinary team or in inter-agency working, that such disclosure takes place on a clear basis of agreed protocols for information sharing.

Recommendation 8

Service providers must establish and ensure the adoption of clear publicly accessible protocols for information sharing within teams, beyond teams and with outside organisations.

Multidisciplinary work. Healthcare professionals as part of their work will have contact with other professionals and other agencies delivering aspects of care. Healthcare professionals may have different criteria and thresholds for the disclosure of confidential information, for example in relation to public safety. It is essential that each healthcare professional familiarise him or herself with such differences and moderate disclosures accordingly.

Guidance Point 14

The healthcare team may include temporary members for particular functions and the healthcare professionals must not disclose information to temporary members unless they are under a sufficient obligation of confidentiality for that level of disclosure.

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

Healthcare professionals may have different criteria and thresholds for the disclosure of confidential information, for example in relation to public safety. It is essential that each healthcare professional familiarise him or herself with such differences and moderate disclosures accordingly.

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

Guidance Point 15

Where it is planned to involve staff from other agencies this should first be discussed with the patient and/or their legal representative. The purpose of involving the other agency should be clarified along with the purpose of the contemplated information sharing.

Where a patient or their legal representative refuses to consent to the involvement of other agencies their refusal should be respected unless there are overriding interests. (See Guidance Points 19-23.)

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

3.2.6 Dual roles and obligations

Healthcare professionals may work in situations where they may have dual roles with dual and conflicting responsibilities and obligations. This includes work in prisons and for court liaison schemes where there are duties to both the patient in their care and to the authority. Such dual roles and obligations may cause conflict about the confidentiality of patient information. For example, a prisoner or defendant may have consulted the healthcare professional and divulged information that they do not wish an outside agency to know, while in their current role the healthcare professional may be obligated to disclose that information.

Recommendation 9

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

Guidance Point 16

Healthcare professionals should avoid situations with dual responsibilities and obligations to the same patient wherever possible.

Where a healthcare professional has dual responsibilities it is important that they explain at the start of any consultation or assessment to the patient and/or their legal representative 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 and/or their legal representative that the information given will not be treated as confidential.

3.3 Protection, Use and Disclosure of Patient Information for Healthcare Purposes not Directly Related to their Healthcare

Many uses of confidential healthcare information not directly related to the healthcare of the patient are legitimate for limited and specified healthcare purposes provided certain criteria are met. In particular, patients and/or their legal representatives must be kept informed of all such anticipated uses, their express consent gained for such uses, and all such uses kept to the minimum necessary. A possible exception to the requirement of

gaining consent for a particular secondary use would be where a legal obligation to disclose for that purpose exists (see 3.4.1).

Secondary uses of confidential patient information are uses in healthcare which do not contribute directly to or support the healthcare that a patient receives. Such uses are increasingly required for evidence based practice and a rational approach to service planning, management and commissioning. The following are some examples of secondary uses:

- planning of services;
- payment for services;
- management of services;
- contracting of services;
- risk management;
- patient safety;
- investigating complaints;
- auditing accounts and performance;
- local and national inquiries;
- teaching;
- research.

Many administrative and management uses of confidential patient information are essential to the provision of healthcare in modern societies. However, research to develop healthcare is not itself healthcare and the two situations must be treated differently when considerations of privacy and confidentiality arise.

The development and increased use of Information and Communication Technology (ICT) have increased the opportunities for secondary uses of patient information. The establishment of large medical databases extracted and aggregated from individual clinical data can be used to enhance healthcare evaluation and public health surveillance. They can be used for example to trace long-term effects of medication, courses of particular diseases and outcomes of specific medical interventions. The protection of confidentiality and respect for privacy rights contribute to the development of such databases by helping to ensure that patients or their legal representatives are willing to provide the information in the first place.

Secondary uses of patient information raise concerns about confidentiality. Practice varies as to how patient information is used, what procedures are followed to ensure confidentiality and where responsibilities lie. The introduction of ICT to assist administrative and wider secondary uses raises additional concerns. Paper based medical records typically do not move much beyond the primary location where patient care is delivered and they are maintained locally. However, extracting patient information from such records on to other systems, particularly electronic, can lead to widespread dispersal of patient identifiable information. While the use of electronic

media raises particular concerns (such as large centrally held databases), the same technology also offers solutions to such problems.

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

3.3.1 Keeping patients informed about secondary uses

All health service organisations must have policies for informing patients and/or their legal representative of the protections, uses and disclosures of their information for secondary purposes. Patients and/or their legal representative must also be informed of the categories of people and organisations to which information may need to be passed for health services to function. Patients and/or their legal representative 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 and/or their legal representative that they may object to specific secondary healthcare uses of identifiable patient information and that their objection will be respected.

Recommendation 10

Health providers must ensure that patients and/or their legal representative are informed of all proposed secondary uses of their information and that they are aware of their choice on such issues.

3.3.2 Consent for secondary use or disclosure of confidential patient information

Express consent from the patient or their legal representative should wherever possible be obtained before any proposed secondary uses of patient personal information. Where there is agreement to disclosure, only the minimum necessary patient identifiable information should be used for each legitimate healthcare purpose.

Guidance Point 17

Express consent from the patient or their legal representative should where possible be obtained before any proposed secondary uses of their personal information. Where there is agreement to disclosure, only the minimum necessary patient identifiable information should be used for each legitimate healthcare purpose.

Possible justifications for not seeking consent for a secondary use of patient information are that it is impracticable or impossible because of particular circumstances. These grounds for not seeking consent for a secondary use of patient information can be considered as follows:

(a) It might be *impracticable* to obtain consent for the use of patient information for a secondary use (for example a public health study) where the patient information had been obtained some time previously. A possible ground for justifying not obtaining consent would be disproportionate effort (for example obtaining consent for a large sample of patients on whom the information had been obtained many years earlier).

(b) It might be *impossible* where the confidential information was obtained with consent for a particular secondary use, and the potential for use for another purpose is now being considered. If the data has subsequently been irretrievably unlinked from those who initially gave consent, then although they have a moral interest in its further use, gaining their consent to the second use is impossible. Likewise, previously gathered information may have a value beyond the death of the individual. It is sometimes impossible to gain consent for the secondary use of information from a patient who lacks decision-making capacity but in such circumstances there are additional protections which must be observed. (See section 3.1.2)

Independent data protection officers or Ethics Committees should be involved whenever judgments of impracticability or impossibility are given as grounds for secondary uses of confidential information without receiving consent. It is also appropriate for such prior independent checking to occur whenever there is any claim of exemption from the duty to provide information to patients and/or their legal representative about uses or disclosures.

Recommendation 11

Independent data protection officers or Ethics Committees should be involved whenever judgments of impracticability or impossibility are given as grounds for secondary uses of confidential information without receiving consent. It is also appropriate for such prior independent checking to occur whenever there is any claim of exemption from the duty to provide information to patients and/or their legal representative about uses or disclosures.

3.3.3 Maintaining information in a form which protects the identity of the patient

Personal information should wherever possible be maintained in a form that protects the identity of the patient from disclosure to unauthorised persons.

Recommendation 12

Personal information should wherever possible be maintained in a form that protects the identity of the patient from disclosure to unauthorised persons.

Recommendation 13

Organisations providing healthcare must have formal information protection agreements with any other organisation with whom it is proposed that information be shared. There should be clear institutional policies on protecting confidential information in a situation where no such agreement exists.

Guidance Point 18

Healthcare professionals should strive to ensure that appropriate policies and protocols to protect the identity of the patient are in place and operational in their hospitals and units and among commissioners of services for secondary healthcare uses of patient identifiable information.

3.3.4 Use of information for teaching purposes

Not only healthcare professionals, but also students in healthcare training have obligations of confidentiality. In addition to meeting the general requirements for secondary uses of patient information, training providers must ensure that students are aware of their obligations of confidentiality and the consequences of any breaches.

Recommendation 14

In addition to meeting the general requirements for secondary uses of patient information, training providers must ensure that students are aware of their obligations of confidentiality and the consequences of any breaches.

3.3.5 Anonymisation for research uses

Anonymisation does not provide an alternative to the gaining of express consent, but rather an additional protection for what remains confidential information which is only legitimately used or disclosed with consent. Anonymisation, as understood by the Data Protection Directive, places data outside the reach of the data protection principles of the Directive. As such, administrators and researchers have a special interest in being able to claim the data they are processing has been rendered anonymous in the terms of Recital 26 of the Data Protection Directive. However, in these terms, personal data is only rendered anonymous if it is no longer possible for anyone (the data controller or anyone else) to identify the data subject from the data itself or from this in combination with any other means that offer a reasonable likelihood of being able to reveal the identity of the data subject. Thus, for example, where a researcher holds data in a form that does not enable the researcher to identify the data subject, but someone else holds a code that enables that person to do so, the processing done by the researcher is not processing of data rendered anonymous. However, it is not unknown for researchers to claim that they are processing anonymised data when others, or even they themselves, can identify the data subject by various straightforward means. For example, researchers

usually describe any data that does not 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 Ethics Committees and data subjects to decide what significance that has.

Where someone intends to render information genuinely anonymous, they can best ensure that they act legally and ethically by informing patients and/or their legal representative of their intention to do so and the effect that this will have, specifically on the ability of patients to access their data and to know what it is being used for (and hence to object to such uses). This is because the Data Protection Directive requires data subjects to be informed of the purposes of all processing of personal data and rendering data anonymous is itself a process performed on personal data. Furthermore, such prior informing should not be used as an excuse not to inform data subjects of the purposes of intended processing of data after rendering it anonymous. Anonymisation should be used in situations 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 19

Information should only be kept in forms that enable the patient to be identified if this is necessary for the purposes for which it is being kept. Data which has been rendered anonymous means that the patient can no longer be identified directly or indirectly by anyone from that data. Whenever it is intended to render data anonymous, patients and/or their legal representative must be informed by the healthcare professional of this intention 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. Patients and/or their legal representative should be informed of the purposes of the intended processing of data after it has been rendered anonymous.

3.3.6 Research databases containing personal identifiable information

Specific considerations apply where identifiable patient information is to be stored in databases as a resource for research and where such information is to be used as research data by researchers other than those involved in the patient's care. Information can be stored in databases in several forms, including hardcopy, digital records and biological samples. Patients' privacy rights and confidentiality must be respected regardless of the form in which the information is held.

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 collecting information. 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 and consultation 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 individuals for the inclusion of their confidential information in that database. The population can withhold democratic consent communally, but consent for the inclusion of information can only be given individually.

In those situations where it is impossible to foresee a potential research use of confidential information at the time of collection, it is difficult to meet the requirements for informed consent without re-contacting participants. This can be both a nuisance for participants and a serious hindrance to database research. A general consent may permit research use of the personal information, where potential participants are initially properly informed about general details of the database including the following:

- what 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 their data will only be used for specified healthcare purposes;
- the data will be used for the research of named diseases;
- who will be likely to benefit from the research;
- who will profit financially from the research;
- that participants will be regularly informed if they wish about the research; and
- that they can opt out of the research at any time if they choose.

Recommendation 15

For those situations where it is impossible to foresee a potential research use of personal identifiable information as part of a database at the time of collection, it is essential that the initial consent to including participants' data include consent to limited conditions for use of the database, specifically healthcare purposes and named diseases.

All database research should be ethically reviewed. The Research Ethics Committee should judge what research is sufficiently important, as well as what precautions are necessary to protect the information of participants, within the limits of national and international legal regulations. Research Ethics Committees should also decide when participants need to be contacted again (for example, when proposed research differs from the initial conditions for use).

Recommendation 16

All research using databases of personal identifiable information should be independently ethically reviewed. In particular, the independent ethical reviewers

should decide on the permissibility of new research uses and the necessity for recontacting research subjects.

3.4 Obligations and Justifications for the Disclosure of Patient Identifiable Information for Purposes not Related to their Healthcare

In some situations, healthcare professionals might be under a legal obligation to disclose information, or disclosure might be legally justified. Where a legal obligation to disclose exists, non-disclosure might have legal consequences. A legal justification of disclosure, on the other hand, means that while the healthcare professional does not have to disclose confidential information, disclosure might under certain circumstances be regarded as legally acceptable. Every disclosure must also be ethically acceptable.

3.4.1 Legal obligations to disclose

In a number of 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. The healthcare professional must bear in mind that failure to do so may lead to legal sanctions. However, given that every disclosure is an interference with the patient's right to privacy, disclosure should not be made uncritically and should be kept to the absolute minimum.

In some European countries courts and other authorities that have a legal right of access to certain confidential information have powers to order the disclosure of documents before and during proceedings. They can also 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. A healthcare professional of a defendant can also be compelled to answer questions about what the defendant has said to them, as well as providing details of the patient's medical history and condition. The healthcare professional must do his or her best to ensure that every argument that can properly be put against disclosure is put before the court. Any disclosure must be limited to what is strictly relevant to the court proceedings.

Guidance Point 20

Where in the course of the healthcare professional-patient relationship a legal obligation to disclose is clearly becoming relevant, this should be discussed with the patient and/or their legal representative as early as possible unless such discussion would itself undermine the purpose of the disclosure. Before complying with any possible legal obligation to disclose, healthcare professionals must satisfy themselves that the situation clearly falls under the category of cases for which disclosure is legally required. They must ensure that every argument that can properly be put against disclosure is put

before the authority to which disclosure needs to be made. Any disclosure must be limited to what is strictly necessary.

3.4.2 Justifications to disclose

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 violates 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).

In all of these cases, there is no obligation to disclose, but whether or not disclosure can be justified rather depends on balancing the interests that are in conflict in each case. It needs to be borne in mind that every instance of disclosure leads to a certain violation of the patient's right to privacy, while the benefits of disclosure will often be less certain. While a balancing of the patient's right to privacy against other rights and interests is always difficult, it is usually more easily performed where the conflict is with rights of identifiable third parties, than where there is a conflict with a more diffuse public interest such as national security or public health. It is not sufficient that it might be more convenient for the protection of such interests that information is disclosed, but the test is instead one of strict necessity in the specific circumstances of each case.

Guidance Point 21

Healthcare professionals should ensure that they are aware of any country specific legal provisions or principles according to which the weighing of interests needs to be performed.

Guidance Point 22

In situations involving disclosure to protect overriding rights of third parties, each case must be considered on its merits. The test is whether the release of information to protect the interests of a third party 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 balanced judgement.

Factors to consider when reaching such a decision are, among others:

- the importance of the interest that is at risk without disclosure, for example disclosure might be more easily justified where the life or integrity (physical or psychological) of a third party is at risk;
- the likelihood of the harm occurring in the individual case, that is, disclosure might be justified where there is a high likelihood of harm to the life of another, but not necessarily justified where there is a low likelihood of harm;
- the imminence of the harm, that is, disclosure might be justified where protection of the third party requires immediate action, but not where there is no more than a possibility that at some future point the patient might pose a threat to another;
- the existence of a sufficiently appropriate authority to whom disclosure can be considered;
- the necessity of the disclosure to avert the harm, that is, that there is no possibility of averting the harm without disclosure;
- the likelihood that disclosure can avert the harm, which requires that the healthcare professional be satisfied that the harm to the third party or to the legally protected public interest is sufficiently likely to be averted by disclosure.

Disclosure to protect the best interests of the patient. Disclosure to protect the interests of the competent patient against his/her wishes can never be justified, as on balance, the right of the patient to decide autonomously what is in his/her interests always prevails.

Where the patient is incompetent, disclosure can be justified to protect the best interests of that patient. Whether disclosure is justified in the individual case depends on a careful weighing of the patient's interest in having the confidentiality of his/her information maintained and the interests that are at risk without disclosure.

Guidance Point 23

Where a patient is incompetent, disclosure can be justified to protect the best interests of that patient. Whether disclosure is justified in the individual case depends on a careful weighing of the patient's interest in having the confidentiality of his/her information maintained and the interests that are at risk without disclosure.

Good practice for justified disclosures. When a decision has been reached that disclosure is justified in a particular situation, there are requirements for how that disclosure should best be made.

Guidance Point 24

In all instances where judgment is involved, healthcare professionals are urged to discuss the case with colleagues without revealing identifiable details of the patient and, if necessary, to seek legal or other specialist advice.

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 to disclose has been reached the usual procedure would be as follows:

- an explanation of the reasons for sharing information should be given to the patient and/or their legal representative;
- the healthcare professional should encourage the patient (and/or where appropriate, their legal representative) to inform the relevant authority (for example, police or social services). If the patient or legal representative agrees, the healthcare professional will require confirmation from the authority that such disclosure has been made;
- if the patient or their legal representative refuses to act, the healthcare professional should then tell them that he or she intends to disclose the information to the relevant authority or person. He or she should then inform the authority, disclosing only relevant information and make available to the patient and/or their legal representative the information that he or she has released; and
- healthcare professionals who decide to disclose confidential information (with or without prior informing of the patient and/or their legal representative) should be prepared to explain and justify their decision to the authority if called upon to do so. The healthcare professional 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.

The exception to this normal procedure is where informing the subject of the disclosure in advance that the disclosure will be made would prevent achieving the justified aim of the disclosure.

3.5 The Security of Patient Information

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. A coherent institutional framework for information governance is required. Within such a framework the principal means of enhancing the security of personal information are restriction of access and the maintenance of information in a form which protects the identity of the patient.

Guidance Point 25

Given the healthcare professional's responsibility to maintain patient confidentiality, professionals should strive to ensure that appropriate policies and protocols are in place and operational in their institutions and among commissioners of services for maintaining the security of patient information.

Healthcare professionals should be mindful of strict privacy and security obligations when communicating with patients, their legal representatives, carers and colleagues, particularly where indirect methods are being used such as telephones, e-mails and faxes.

Glossary

Anonymisation. According to Recital 26 of the Data Protection Directive, to render personal data anonymous places it outside the scope of the Directive. For personal data to have been rendered anonymous it must no longer be possible for anyone to identify the person who is the subject of the data directly (that is, from the data itself) or indirectly (that is, from the data itself in conjunction with other data or means that are "reasonably likely to be used", such as an identification number or to one or more factors specific to the subject's physical, physiological, mental, economic, cultural or social identity). Coded and encrypted data is not anonymous for the purposes of European data protection law if anyone can decode or de-encrypt it without unreasonable effort.

Best Interests. A standard according to which decisions are made on behalf of incompetent patients.

Capacity. Laws specific to each country define the requirements for someone to have the mental capacity to make a decision as well as the place for a proxy to have the authority to take a decision on behalf of the patient.

Carer. A term used to include a variety of people that range from parents to relatives or professional carers who, while caring for the person, may not have any legal authority to have access to their information.

Clinical Audit. The process of comparing actual clinical activity undertaken and outcomes against standards to measure achievement and identify mechanisms for improvement.

Consent. Three conditions must be satisfied for consent to be effective. First it must be informed. A patient (or their legal representative) cannot be considered 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 to provide them with appropriate care. Second, it must be given freely and without duress. Third, there must be some indication that the patient has given consent. This may be express (explicit) or implied (implicit). Valid consent requires that the patient has been provided with information as to what information it is intended to disclose, and for which purposes disclosure is suggested. Consent also presupposes choice, which means that the patient who is asked to consent must have the possibility to refuse to give such consent or to withdraw such consent.

Council of Europe. The Council of Europe is the continent's oldest political organisation, founded in 1949. It groups together 46 European countries and is distinct from the 25-nation European Union, but no country has ever joined the Union without first belonging to the Council of Europe. The European Convention on Human Rights

and related international instruments come from the Council of Europe. See http://www.coe.int for further information.

European Union. The European Union (EU) is a union of twenty-five independent states (as of 2005) founded to enhance political, economic and social co-operation. See http://europa.eu.int for more information.

European Court of Human Rights. The European Court of Human Rights is an international court based in Strasbourg. The Court applies the European Convention on Human Rights. Its task is to ensure that States respect the rights and guarantees set out in the Convention. It does this by examining complaints lodged by individuals or, sometimes, by States. Where it finds that a member State has violated one or more of these rights and guarantees, the Court delivers a judgment. Judgments are binding: the countries concerned are under an obligation to comply with them.

Healthcare Professional. Includes, doctors, nurses, psychotherapists, physiotherapists, occupational therapists, radiographers etc. Anyone who provides healthcare directly to the patient.

Healthcare Purposes. Activities undertaken for healthcare purposes are those with the aim, directly or indirectly, of improving health or reducing illness in individuals or groups.

Healthcare Information. Includes information about a person, regardless of the form in which that information is held.

Intellectual Disability. The current WHO diagnostic term is '*Mental retardation*' but, although in use in the Americas, is unpopular and has been replaced with '*Mental Handicap*' (in much of the EU) or '*Learning Disabilities*' (in the UK).

Legal Representative. A person provided for by law to represent the interests of, and/or take decisions on behalf of, a person who does not have the capacity to consent.

Patient. Any person receiving healthcare from a healthcare professional.

Primary Uses. Primary uses of confidential patient information are uses in healthcare which contribute directly to or support the healthcare that a patient receives.

Principle. A basic rule that guides or influences thought or action.

Public Interest. Legal justification for the disclosure of confidential information in order to protect an overriding interest of members of the public or the public as a whole. In many jurisdictions this legal justification will often be provided on the basis of necessity.

Secondary Uses. Secondary uses of confidential patient information are uses in healthcare which do not contribute directly to or support the healthcare that a patient receives.

EuroSOCAP Project Board

European Guidance for Healthcare Professionals on Confidentiality and Privacy in Healthcare

Introduction

All patients have the right to privacy and the reasonable expectation that the confidentiality of their personal information will be rigorously maintained by all healthcare professionals. Each patient's right to privacy and the professional's duty of confidentiality apply regardless of the form (for example, electronic, photographic, biological sample) in which the information is held or communicated. This guidance applies to all healthcare professionals and addresses the areas of healthcare confidentiality and informational privacy. It forms part of the European Standards on Confidentiality and Privacy in Healthcare which elaborate this Guidance and provide Recommendations to healthcare provider institutions, based on ethical and legal foundations. The Standards also contain a Glossary. The text of the Standards and the Guidance are available in various languages at www.eurosocap.org.

The European Standards are primarily ethical standards, developed within the legal context in which healthcare professionals make decisions about the protection, use and disclosure of confidential information. Not all healthcare professionals are bound by the same legal obligations of confidence, but all are under the same ethical obligations to maintain confidentiality.

The Guidance gives detailed consideration to the needs of vulnerable patients. The needs of vulnerable patients are greater with respect to confidentiality—there is greater risk of it being breached than is the case for other patients. Particular care is needed on the part of healthcare professionals to ensure that the right to privacy of vulnerable patients is respected and that their duty of confidentiality toward them is fulfilled.

In this Guidance three areas of protections, uses and disclosures are considered:

- protections, uses, and disclosures of patient information for their healthcare;
- protections, uses, and disclosures of patient information for healthcare purposes not directly related to their healthcare; and
- obligations and justifications for the disclosure of patient identifiable information for purposes not related to their healthcare.