The Good European Health Record

Ethical and Legal Requirements

Deliverable 8

19 October, 1993

Local document name: ETHICS4.DOC

Table of contents:

Scope of document:

This document addresses the ethical issues raised by application of information technology (IT) to the medical, patient, clinical or health record. The term health care record is preferred as it does not include connotations that the use of the record is confined to doctors. The term health care record is reserved for that part of the record which is only created by clinicians. Any reference to the administrative information will be made specifically. The term electronic health care record (EHCR) is used when referring to the health record created and stored on computer. It is the equivalent to the computerised patient record (or CPR) in the American literature.

A large number of ethical issues are raised by the application of IT to personal data. Some of these relate to system security, some to processing, and many to the competence or good practice of the user. The interaction of these aspects is complex and problems may have many causes. For example, a user may invoke a process (which may or may not give the expected result) for which they did not have access (due to a security fault) and then distribute the result because they were not adequately trained, or the security policy of that institution was not publicised.

We have made statements in this document, which some readers may not feel have been justified or argued adequately. They have been the concern of documents previously published (GEHR 1991, CEC 1992). With this in mind we have assumed that:

- regulation is necessary in this domain.
- application of IT to the health record is an appropriate step which will lead to an improvement of patient care.
- design of systems can be consistent with moral and legal requirements.

The main concerns of this document fulfil the following criteria:

- There is a risk of serious harm to patients or clinicians.
- The risk involves the health care record and its processes.
- The risk can be minimised without compromising the usefulness of the record.
- Regulation is both technically feasible and morally appropriate.

The boundary and purposes of the health record

When considering the EHCR, it is necessary to know what an EHCR is and what it is for! While it is not the place of this document to define these concepts, it is necessary to agree on a working definition.

The boundary of the EHCR

The Good European Health Record Project and other projects of the AIM programme in

Europe and the Institute of Medicine and others in the USA are developing the concept of an electronic health care record. It is, however, important to accept that if a patient is to have control over something, and if a clinician is going to be accountable for the use and content, then it must be absolutely clear to all parties what is and what is not the health care record. For the purpose of this document it is all recordings made by a responsible clinician regarding the care of that patient. Thus information does not form part of the health care record until a clinician had taken responsibility for that information and entered it into the record.

The purpose of the EHCR

particular purpose of the health care record is to some extent dependant on the health care facility (HCF) and the health care offered. There is, however, broad agreement that the primary purpose is to benefit the patient by making a record of care that supports the provision of care by the same or another clinician in the future. The secondary purpose of the record is to provide a medico-legal record of the care provided, should there be any reason to investigate the competence of the clinicians providing care. Hence the secondary purpose of the record is to demonstrate the competence of the clinicians. The tertiary purpose(s) of the record must be legitimate (involve consent), and must not jeopardise the primary and secondary purposes. Purpose can be seen in terms of benefits. The purposes of the EHCR may be summarised as in the table below with the major beneficiary as heading.

Patient	**Clinicians**	**Other Third Parties**
basis for Clinician's accountability basis for HCFs' accountability	a working tool a legal document basis for communication storage of patient oriented objectives collectively oriented objectives	basis for health statistics

Thus a health care record can operate in the interests of a number of people and has potentially a wide audience. It is a key element in individual care, acute and preventative care, in supporting and authorising clinical care and decision support. It provides the basis for liability in case of negligence, and is a source of health care statistics.

Glossary:

Certain terms are defined at the outset of this document, and will be used throughout the document in a consistent manner, in order to minimise the potential for confusion. It is clear that we must agree a common understanding of the key concepts involved, and these definitions have been taken from the formalism developed for information structure.

The parties involved with the Health Care Record:

When stating moral principles, it is necessary to describe the real world in an unambiguous way. In order to achieve this and acknowledge the diversity of health care practice in Europe, it has been necessary to define all people and places in terms of the health care record. When terms are used with these specific meanings ***they appear in italics***. These meanings are specific to this document.

The Patients' world:	
Patient	The individual person with whom the health record is identified. For every patient at a *health care facility* there is at least one health record.
Next of Kin	The named individual in the health record who has been nominated by the *patient* to make decisions on their behalf if they are unable to make them competently. The *next of kin* may or may not be a *carer*.
Carers	People who provide lay care to the *patient*, expressed by the willingness of the *patient* to share some or all of the contents of the health record with the *carer*.

The Clinicians' world:	
Clinician	Any person whose involvement with a *patient* involves provision of care and a duty to record that care in the health care record.
Non-clinicians	Any person whose involvement with a *patient* involves provision of service and no duty (or a duty not) to record that care in the *patient*'s health care record. The *non-clinician* may make entries in the administrative part of the health record. The EHCR must contain an administrative section in which both *clinicians* and *non-clinicians* may make recordings.
Responsible clinician	The *clinician* who makes a particular recording in the notes and who accepts responsibility for the care documented, and the accuracy of the recording. The recording may in fact be transcribed by a secretary, but each clinical recording will be identified with one *responsible clinician*.
A Health Care Facility	An organisation which maintains a store of *patients*' health care records (HCF)
Clinical Student	A student in training for a profession which has clinical status in that *health care facility*, and has an accepted need to access *patient* health records.

Third Parties:	
Controller	The person legally responsible for the health care record stored on computer, and for processing of the record.
Technologist	Person involved in the development, operation and maintenance of the EHCR and supporting hardware.
Administrator	Person administering and planning for *health care facilities*. *Administrators* provide no direct service to *patient*s except in unusual circumstances.
Legal professional	Person with legal qualifications who has a need to access medical records.
Other third parties	Other people who may receive information from the health record.

Words used to describe the clinical record

Many legal and ethical considerations have been taken into account when describing the clinical requirements (GEHR 1992) and the specification of the electronic health care record (GEHR 1993). Some terms are used in this document that have been defined previously and are used again with the same meaning. These terms **'appear in single quotation marks'**.

Consultation	An encounter between a health professional and a patient, in which health information is acquired or exchanged. This process may be recorded in one or more transactions.
Transaction	A recording within an EHCR, which relates to a single patient, a single date and time, a single responsible person, and is committed permanently to a particular part of the record.
Definitions of transaction types:	

Administrative	This transaction type will be used to record any information which assists in the management of a patient but which is not specifically related to their health status e.g. name and address. Any health care worker, including clinicians can be responsible for this transaction.
Contact	Any information that relates to a provision of care by clinical staff will be recorded within a contact transaction. This type of record entry is also known in the literature as **Encounter record** or **Progress note**. They may or may not always see the patient as a recording may arise from the clinician receiving a test result or a letter and recording an opinion or proposed action. It may often be necessary to define further the type of consultation, the location of the consultation, the type of clinic, or other specific information relating to it. This should be stored in the transaction definition.
Summary	Any information that is deemed to relate to the past provision of care for that patient or patient's relatives which has a relevance beyond any single transaction will be recorded within a summary transaction.
Trigger	Any condition or information requiring action at a future date, or circumstance. It may require mandatory elements such as the date and time for this information to brought to the carers attention, the date and time the action falls due, the relationship between the information and the date (e.g. no later than, no earlier than etc.).

Report	These transactions are reserved for information which has a legal status outside the record. Thus report transactions involve communication from one responsible person to another. Clinical letters, requests for and results of tests, would be examples of this.
Continuing Care	Transactions of this type are reserved for information which has relevance for future transactions, relating to the continuing clinical care. In some ways it will resemble a summary transaction, except relating to the future rather than the past, and therefore more liable to reviews and changes.
Nota Bene	This transaction type will be defined by its behaviour, as the information will be displayed whenever the record is opened. It is thus critical information relating to this patient, which the last clinician requires the next clinician to see.

Chapter One.

Introduction : The Importance of Moral and Legal Regulation of a good Electronic Health Care Record (EHCR).

The Problem

Both in Europe and elsewhere the Electronic Health Care Record (EHCR) or computerised patient record is increasingly used in clinical care. This is principally because developments in information technology (IT) allow a "paperless office". The EHCR must still fulfil the two major roles of the traditional medical record - supporting the care of the patient and providing retrospective evidence of competent care. However it differs fundamentally from the paper record. The EHCR is stored on a different medium (i.e. magnetic or optical) in digital format and cannot be read without the assistance of technology. It can be seen or used in more than one physical location at the same time. It can be copied and an identical replica created which cannot be differentiated from the original. It can be processed automatically. Many practical consequences arise from such differences.

As is the case with most dramatic technological innovation, the EHCR has developed with little social regulation. Interested clinicians and information scientists have produced a plethora of designs and implementations using different tools and hardware. The result is an inability to pass records on to other sites. The next generation of electronic health care records - like the Good European Health Record - has new aims. These are driven by political and economic policies as well as by motivated clinicians and information scientists.

The European Community has generated an international political will to develop health care with a broad focus involving shared standards which implies shared records. The mobility of people is itself reason to establish a 'borderless' medical record, particularly as this movement involves both *patients* and *clinicians*. The effective care of tourists and workers from different countries, in the context of increasing use of IT, depends not only on the 'physical' access to information regarding the *patients*' health, but equally on familiarity with the structure and function of the EHCR. A true 'borderless' EHCR will involve the added formal process of accurate language translation.

Economic pressures exist, brought about by a general will to improve value for money. Health care consumes major economic resources in all developed countries and is of the order of 10% of GDP in most countries. Investment in Information Technology (IT) by hospitals and other *health care facilities* is already considerable[1] and the application of IT to the major data handling function (medical records) has been an aim of *administrators* and some *clinicians* for many years. The use of IT in fields such as health care, with major data handling requirements, is seen as a priority by managers as many have experienced

[1] The average UK hospital spent £520,000 on IT in the financial year ending April 1993. British Journal of Health Care Computing & Information Management. Sept 93 10(7); p5

consequent improved efficiency in other management roles. Efficiency is the aim and once computerisation has occurred manual processes cannot be sustained if the system fails (Barber 1991:346). There is a political commitment to fund these developments in many countries, often specifically within the health care domain.

These political and economic pressures, combined with a general perception that patient care will improve with information flow (Allaërt 1992), have led to the funding of prototype EHCRs which can be shared at different sites and transferred easily between countries. The attendant risks to individual privacy and patient safety are potentially so overwhelming that the Commission of European Communities has seen fit to direct that member states prohibit the processing of health data (CEC 1992:77) The regulatory focus is then upon exemptions, the aim being specific legislation on acceptable processing of health data.

The dangers of abuse of new technology

The application of any new technology carries risk. This risk may not be obvious to the developers who are concerned with the perceived benefit that motivated their innovation. The hopes and aspirations of the politicians, managers and *technologists* for IT applications in health care are matched by fear and anxiety amongst some *clinicians* and *patient*s that the technology will not be implemented or used in a way that has their interests at heart.

Major innovation inevitably begins in a legal vacuum. The motor vehicle and nuclear technology are examples in industry. Invitro fertilisation and embryo experimentation are recent medical examples. In the future, genetic engineering is likely to require regulation pertinent to industry and health care. Regulation is necessary in any area of innovation with widespread application. The arguments for regulation increase with the risk for potential harm to individuals or society. There is, therefore, a prima facie argument for regulation of the application of IT to the health record. It contains highly personal information and the contents are used to make judgements about *patient*s' care. These can involve two kinds of risk: those imposed by the information system and those by the users.

Regulation and technology:

After development of the motor car, there were problems with both the security (e.g. the brakes and handling) and bad practice (no rules of the road). Initially this led to very simple and restrictive regulation - walking with a red flag. This has now become complex with a code of behaviour which allows more flexibility in how and where we drive our cars. Security features, such as locks, good brakes and seat belts have also been developed and at times imposed through legislation.

There is already evidence of abuse of IT in other domains. A recent survey by the UK's Audit Commission found 118 cases of fraud or abuse involving 1200 institutions using IT applications. Another in 1990 showed a further increase in fraud This survey revealed that the most common way of detecting abuse was by inquiries from data subjects. Such a scenario in health data storage is unacceptable, as inappropriate patient care is likely to be the outcome. An increasing percentage of abuse goes undetected for many years. The number that is never detected can only be estimated.

The major potential for abuse is unauthorised access and sabotage, particularly when the system is networked and there is telephone access (Dick 1991:178). This has proved true in small sites in inner cities where theft of computers is not uncommon. The threat of unauthorised access and sabotage predominantly relates to *technologists* as they are able to bypass security. The state of course may also be involved.

The threat of bad practice is more difficult to quantify. Privacy violations are unlikely to be reported by the victims in view of the threat of further broadcasting (Pearce 1988:5). Experience in Canada is not reassuring (Robinson 1992).

> In Canada in September 1990 the Minister of Fitness and Health for Nova Scotia was charged with accessing and releasing information from the psychiatric treatment record of a former government official.
>
> In 1991 the Minister of Health for Ontario resigned after inadvertent public disclosure of the identity of a patient who had been treated for drug abuse. (Robinson 1992)

The information held in the EHCR may be of such a sensitive nature that publication may jeopardise the *patient*'s ability to choose or maintain their present lifestyle. The potential for bad practice is not restricted to the EHCR, as reports of doctors falsifying or even burning paper records[2] remind us. However confidentiality is at far greater risk in an environment where data may be copied and transferred anywhere in the world in seconds. While there is consensus on confidentiality, based largely on the codes of practice established with paper records, the methods for guaranteeing it are not at all certain.

The EHCR poses further threats that are more substantial. These arise as a consequence of the ability to process information automatically and merging information from many sources. The Commission of European Communities (CEC 1992:17) directive states that the context of processing poses the greatest threat to privacy. There is growing concern regarding decisions that affect people being based on automatic processing (Turn 1991:395,CEC 1992:26). Such non-objective decision making is now illegal in France. The risk to *patients* may be greatest in medical applications (CEC 1991:14) as many *clinicians, non-clinicians,*

[2]UK Sunday Observer 21/5/89

administrators and planners, and *other third parties* defend uses for the record not related to providing care for individual *patients* (e.g. epidemiological research, financial planning or medical audit). Many or all of these functions involve automated processing of data, often with linking to other data such as census or financial data.

The ability of a *clinician* to provide high quality care may be compromised by an implementation of an EHCR that restricts the *clinician's* capacity to retrieve information. This problem includes aspects of security- is the information complete, is the system working? - but extends to the *clinician's* ability to use the record properly. This implies a duty to educate and train users.

The potential abuses of IT may be classified in the following way:

Domain	Potential areas of abuse
State	Constitutional rights Public knowledge of existence Social awareness of effects Regulation
Purchasers providers of Health Care	Security Confidentiality Integrity Availability Verification and accuracy Transparency[3] in: Design Operation Evaluation Objectivity Qualitative evaluation[4]
Individuals	Honesty Copyright

Modified from Gritzalis and Katsikas (1991)

Most of these threats are only containable with the help of *technologists*. Yet *Technologists* are most able to abuse the technology. Do they pose a threat? Will they prove as willing to learn about confidentiality as most people employed in the health

[3] Transparency is the ability of any user to see the information held in a system. If the user has the highest level of access, then they should be aware of all information. A lower level user should be aware of all the information to which they have authorised access. Transparency is a consequence of design, implementation, user interface, on line support and documentation.

[4] Decisions about human beings should not be made on the basis of automatic monitoring, but qualitative means.

sector? They will certainly require education, and a code of good practice (McFarland 1991). Legislation will also be necessary.

Avoiding these abuses in an international setting

How do we avoid these risks, while achieving the aim of the EHCR? The risks exist in a setting where the apparently trivial task of retrieving and processing information may be achieved in seconds and where advances in technology enable us to send digital data all over the world. The very rate of change and development of new technologies means that new threats may be real before they are apparent (CEC 1991, Lobato de Faria 1992).

These risks exist at a time when there is no European harmonisation of legal frameworks, a situation which must be corrected (Lobato de Faria 1992). In the interim, a "borderless" health record will rely on trust and recognition of others' work practices. At present, for example, in the United Kingdom a *patient* has full access to their medical record. In Spain, this is not the case. It is clearly important that information recorded in Spain under one working practice is not accessed by the *patient* when in the United Kingdom. A breakdown of trust internationally will result in less movement of health records and diminish the potential benefit for *patient*s and *clinicians*.

The role of the State in the implementation of the medical record is crucial but no less open to abuses. These must also be specifically controlled.

Ethics and the Law

have established that there are problems with the application of IT to health records, and that the potential for abuse is both widespread and important. The question that remains is what mechanisms do we have for establishing the regulation that is required?

Regulation in our society is at once moral and legal. Laws arise from the moral values endorsed within society at a given time. The degree to which they are consistently obeyed will depend upon this endorsement. Ethics is the main methodology for criticising laws, and reference to ethics is an essential element in designing laws. With reference to data protection, Watson (Pearce 1988:113) states:

> "Legal rights do not create moral rights, and legal regulations and other guidance may authorise more or less access or disclosure of personal information than morality requires or permits."

As legal principles are not well developed in this area and there is little agreement throughout Europe (See Appendix) we will develop and apply moral principles primarily in our arguments. When relevant, legislation will be referred to.

The way forward

Having now outlined the problems, we propose to tackle them in the following way. Chapter

Two aims to establish moral and legal principles appropriate to the application of information technology to the health care record. Chapter Three deals with creation, movement and processing of the whole record and concentrates on control of these operations. Chapter Four deals with the detailed contents of the record and control of access and content. Chapter Five deals with the records role in maintaining accountability in clinical practice and for users and maintainers of the system. Chapter Six stipulates the administrative and technical duties appropriate to a secure EHCR. Chapter Seven outlines the educational responsibilities of managers of EHCR systems. Chapter Eight proposes regulatory activities. Chapter Nine defines a number of "slippery slopes" which indicate how apparently sensible regulation might lead to a greater threat to *patients* and *clinicians* or an unworkable system.

Summary

technology, a new and powerful technology, has been introduced to health care records in a climate of political, economic and managerial pressure to speed development. With a lack of codified moral and technical standards, current EHCRs are unable to pass between institutions, and operate without clear security and safety evaluation. The next generation of EHCRs aim to redress these difficulties thus leading to increased movement of health care records and new threats to *patients* and *clinicians*. The minimisation of these risks will require moral and legal regulation defining good practice and systems security.

Chapter Two.
The Principles Behind a 'Good' Electronic Health Care Record.

What moral principles have bearing on an EHCR?

For clinical medicine to be successful, there must be a relationship of trust and confidence between the *clinician* professional and patient. Otherwise, *patients* will be reticent to present themselves for treatment or to divulge the detailed personal information required for successful diagnosis.

There are two key reasons why *patients* place so much trust in their *clinicians*. First, they believe that their care will conform to a high clinical standard - that their life and health will be protected. And second, *patients* assume that their individual autonomy will be respected - their right to decide their own medical destiny, whatever anyone else might think.

These two principles are generally endorsed by all European professional organisations representing health professionals of whatever kind. They summarise the duty of care to which *clinicians* are professionally and legally obligated to adhere.

Protecting the life and health of patients

Clinicians have an obvious professional duty to provide a level of clinical care that conforms to a high standard. This duty is codified in civil and criminal law as it pertains to professional negligence. If serious harm is caused by what is judicially accepted to be a breach of professional confidence then the *clinician* will be held responsible for appropriate recompense.

Morally, the obligation to provide help to those in serious need is widely accepted to transcend specific patterns of national legislation and judicial precedence. Even though *clinicians* in Europe do not have a legal responsibility to meet such need in those other than their established *patients*, there is little doubt that most would accept that in the face of serious harm, help should still be provided - unless the *clinician* is put at risk in the process.

The duty to meet clinical need (and not to cause unnecessary harm in the process) both are and should be a dominant feature of contemporary medical practice. To the degree that *clinicians* have such a duty, they obviously have the right to exercise it to the best of their ability.

Implications for the management of health records

The moral justification for the creation, storage and processing of health records of whatever kind derives from the fact that they are instrumental for the protection of life and health. Without them, the exercise of the clinical duty of care to a high standard would be impossible and great harm would be caused to those who would otherwise be helped. This help may be in the form of treatment of the individual patient or as a result of information

derived from research on EHCRs.

It is equally the case that such records lose their justification to the degree that they actually or potentially cause harm. This loss can only be mitigated by the degree to which the risk of such harm occurring can be minimised and monitored. The harm in question might concern personal injury resulting from careless or accidental error in some aspect of the management of the record. Other types of harm concern the consequences of information being accidentally or intentionally revealed about *patients*.

Respecting the autonomy of patients and health professionals

Patients trust their doctors for reasons other than just technical competence. They also believe that they will be respected as persons - that they and not their doctor will be allowed to decide what medically happens to them.

To deny *patients* this opportunity is to treat them as a means to the *clinicians* end, however good the consequences may seem to be. To do so ignores the personhood of normal adult *patients* - the fact that they have a basic capacity to make reasoned choices about their individual destiny. If reason is not impaired, it is this capacity that dictates the duty to honour the particularly human right of the individual to informed choice in medicine or in any other area of life. There is no evidence, for example, that most animals can make such choices.

What is 'autonomy'?

The idea that persons deserve respect in their own right - whoever they are and whatever the consequences - is often linked to ideas about the moral importance of the concept of personal autonomy. In one of the classic statements of this importance, John Stuart Mill argued:

> "The only part of the conduct of anyone, for which he is amenable to society, is that which concerns others. In the part which merely concerns himself, his independence is of right absolute. Over himself, over his own body and mind, the individual is sovereign."

Moving on to medicine, Ian Kennedy, for example, consistently emphasises the *patients* right to self determination:

> "'I suppose that, for me, the relevant starting-point in any ethical analysis must be the principle of respect for persons as persons. What this means here is that a doctor has a duty to respect the integrity and individuality of the person before him. A more specific duty derived from this is the duty to respect the person's autonomy."

Raanan Gillon concurs:

> "In most cases ..... of a doctor's dealing with patient (or clients - they are not always patient) not only is there an independent moral presumption that he must respect their autonomy but, even if he is interested only in doing them good, he must generally respect their autonomy in order to do so."

of the most widely used textbooks on medical ethics both here and in the United States is Beauchamp and Childress who state:

> "In recent years virtually all medical and research codes of ethics have held that physicians must obtain the informed consent of their patient before undertaking significant therapeutic or research procedures. These consent measures have been designed largely to protect the autonomy of patient and subjects."

The right to respect for autonomy

exploring the implications of respect for the autonomy of *patients*, we need to look more closely at the concept of a human right. To say that a strict right exists to something is to argue that an entitlement exists which must be taken seriously.

rights are entitlements to specific actions or inactions of others. They may entail being left alone to make autonomous choices about life and life style. These are sometimes referred to as 'civil liberties'. Equally, they may require that others provide goods and services that are necessary in order for civil liberties to be actively enjoyed. To the degree, for example, that welfare rights are endorsed, it will be on this basis.

medicine, both types of rights are important in that they will require inaction of some kinds (e.g. no overt deception in obtaining agreement to treatment) and action of others (e.g. the provision of information sufficient for agreement to treatment to be deemed informed).

we believe that an individual possesses a strict right, then this entails that they have an entitlement that commands respect. Thus a strict right cannot be overridden by the preferences of others, no matter how much they may think it in the best interest of the right holder. Therefore, the degree to which a right is a strict will depend on how unqualified we believe it to be. Certainly property rights are reasonably strict in these terms, along with the duties that correspond to them.

there is also a general consensus that these rights and duties are not absolutely strict. For it is also part of the moral currency of our culture and that my rights end at the point at which they pose a serious treat to the life and health of others. Under these circumstances, it may be morally justified for civil liberties to be breached and for the expression of autonomous choice to be curtailed.

The right to informed consent

, the right of individual *patients* to determine their own medical destiny goes hand in hand with the duty of *clinicians* to respect their autonomy. To the degree to which this right is respected, therefore, *patients* will be consulted about their treatment preference after being provided with correct information about them.

deny such choice of treatment - or non-treatment - would be to claim that doctors should be able to do anything they wish to a patient, irrespective of the risks and the discomfort and despite the *patients* protests. To advocate the right of *clinicians* to do so would undermine, for example, our ability coherently to distinguish between medicine and veterinary science. For it is precisely in the case of the former that therapeutic intervention is accompanied by communication with and choice by autonomous *patients*.

The right to confidentiality

is a clear relationship between the preceding discussion and the moral justification for taking the right to confidentiality as seriously as we do other recognised human rights. Indeed, it follows directly from the rights of *patients* to informed consent. Here, the expression of consent extends to who does and does not have access to their medical records.

breach the confidence of a *patient* constitutes a prima facie violation of their autonomy and can have damaging consequences to clinical practice. Even if *patients* present themselves for diagnosis and treatment, the mere suspicion that what they deem to be secret might not be kept secret would probably be enough to destroy the trust crucial for a successful clinical relationship. For example they would be incapable of giving an accurate case history on which to proceed. Conversely, if *patients* refuse to seek medical advice, they put both themselves and, depending on the circumstances, the general public at risk.

to the principle of confidentiality on the grounds of the inherent respect owed to them as a person is to claim that *patients* have a right to control clinical information about themselves. To the degree to which this is accepted it will mean that no one else can force them to reveal any or all of such information if they choose not to. The only qualification to this is the equally widespread view that no one has a human right to cause serious harm to others, including through respect for rights which they would otherwise possess.

right to confidentiality has always been taken seriously by the medical profession. The Hippocratic Oath says: 'Whatever in connection with my professional practice, or not in connection with it, I see or hear, in the life of men which ought not to be spoken of abroad, I will not divulge as reckoning that all such should be kept secret'. Similar statements of principle are found throughout the contemporary ethical codes of European medical organisations.

, there is a crucial qualification in the Hippocratic Oath which suggests that the morality of respecting confidentiality in professional practice is more complex. Aside from stressing the importance of keeping secrets Hippocrates suggested that confidences could be broken when they ought to be 'spoken of abroad', as he put it. Unfortunately, he does not tell us when

such breaches are warranted.

European codes again endorse this qualification, stating that breaches of confidence can be morally justified in some situations provided that they are in the interests of the *patients* and/or the public.

regards the former, information obviously must be shared among health professionals involved in the *patient*'s treatment. Yet in most circumstances, this can hardly be called a breach of confidence. Their consent to information being shared is implied by their general informed consent to treatment. Of course, *patients* may attempt to forbid clinical information relevant to their treatment being given to an attending *clinician*. However in these circumstances, they cannot have it both ways, assuming that they really do want the best available treatment.

fact, the situations where breaches of confidence can be justified morally in the competent *patient*'s best interest are few and far between. They primarily concern life threatening emergencies where *clinicians* need information from relatives when for one reason or another they cannot get it from *patients*.

breaches of confidence of the second kind - those in the interest of the public - bring us closer to many current debates about the management of ,say, HIV/AIDS *patients*. For here the argument again takes us back to the prevention of serious harm to the public through overriding individual rights which could otherwise be respected. There are a variety of circumstances concerning the individual right to confidentiality within the clinical relationship which are analogous to our reference to private property rights. The entitlement of the *patient* to control all the clinical information which emerges from their diagnosis and treatment becomes equally circumscribed when as a result, the public are placed at risk of serious harm.

example, in most European countries *clinicians* have either the moral discretion or the obligation to breach confidence in the face of such harm. For example, in some (but not all) European countries, a *clinician* might breach the confidence of *patients* who threatens serious harm to another specifically known individual. Further, the whole apparatus of public health legislation and provision for the notification of infectious diseases is based on the same moral reasoning. Finally, *clinicians* have to breach confidence if judicially instructed to do so in the public interest.

all of these situations, the rights of the public to protection from harm - including the rights of insurers - are deemed to trump the rights of the *patient*. There no longer appears to be much disagreement within the profession about this.

Further implications for the management of health records

follows for the preceding argument that morally individuals may be seriously harmed through a violation of their autonomy through either a breach in their right to informed

consent or to confidentiality. Aside from whatever impairment occurs to their autonomy itself (e.g. a loss of confidence to maintain self-affirming patterns of social interaction) the personal implications of such breach can be devastating.

patients believe that they are being manipulated or deceived, clinical trust can be damaged with potentially dangerous consequences. Further, if medical information which is deemed secret is made public the private and professional lives of individual *patients* can be completely disrupted. The consequences for the continuation of the ordinary lives of such *patients* can be potentially just as damaging as the physical illness for which they are being treated.

, *patients* should exercise as much choice over the content and movement of their medical record as is consistent with good clinical care and lack of serious harm to others. Records should be created, processed and managed in ways that optimally guarantees the confidentiality of their contents and the legitimate control of *patients* over them.

principles should be incorporated in all electronic medical records and special efforts are required to insure both their accessibility to *patients* and their security. Here in light of the potential ease of others accessing and transmitting the whole or partial contents of such records, the potential for abuse is great.

problem is that health data has another value. It is potentially valuable to the community. Widespread legislation for compulsory reporting of contagious disease is an example. With automatic processing, the value of data in an EHCR is considerable. Lobato de Faria (1992:358) has stated a widely held belief:

> "The use of computers in health systems poses a well known basic dilemma: the benefits for both medical care and research of easily accessible, reliable and inter-connectable national or even international databases, compared to the privacy risks all these facilities imply."

Health records and the rights of clinicians

have already seen that if *clinicians* are to be able in principle to protect the life and health and respect the autonomy of their *patients* then they must have the right to do so. This right extends to the entitlement to employ health records in ways which are consistent with it.

general, there will be no conflict between the *clinicians*' rights and duties. Usually, the one will mirror the other. However, at times, it will be necessary to act in the best interest of *patients* when they are unable to do so themselves. Equally, there may also be circumstances when respecting the autonomy of one *patient* has to be qualified if the rights of others are thrown into jeopardy. An example of the former might be the necessity in the course of treatment to create or move records of *patients* who have become incompetent for whatever reason. The latter might occur when discretion is used to inform on a very dangerous criminal who has sought medical treatment.

weighing up the balance between the rights and duties of *clinicians* it is important to ground it in as much of a partnership-in-care with *patients* as is practically possible. As regards health records, this entails providing *patients* with control over and access to their records to a degree that is consistent with their safety. At the same time attempts should be made to educate *patients* as to the meaning and medical significance of such records. The exercise of clinical rights will be both easier and most personally gratifying with *patients* who are in a position of a partner in rather than a recipient of clinical care.

What legal principles have a bearing on an EHCR

is close relationship between morality and the law. Moral principles and argument are at the heart of the content and interpretation of legal statutes and case law at any given time. They form the substance of whatever reasons given for the creation of specific statutes and why they are interpreted in particular ways in the face of the differences between individual cases.

This said, there are important differences between what is accepted to be the law and what is believed morally to be right or wrong with it. What is the case legally need not be accepted as what ought to be the case. For example, abortion under restricted conditions is now believed to be legal in a variety of European countries. Yet the moral debate continues to rage as to the acceptability of these conditions. As we will see in later chapters, the same applies to differences of moral opinion about the what constitutes a ’good’ health record, whatever might or might not be viewed as the law.

The majority of legislation and directives from the Commission of European Communities relating to information security are not within the health care domain. In 1992 these related to standards, testing and certification, company regulation, government procurement, harmonisation of regulation and services, and liberalisation of capital movements. Sherizen (1992) states;

> "EC activities are to harmonise legal, administrative and technical requirements for the establishment of an information market and to establish greater standardisation and simplification."

The AIM Requirements Board (AIM 1989) have developed six safety first principles for the environment in which a health record should operate:

1. Safe environment for *patients* and users
2. Secure environment for *patients*, users and others
3. Convenient environment for users
4. Legally satisfactory environment across Europe for users and suppliers
5. Legal protection of software products
6. Multi-lingual systems.

It is clear to any observer that the legal diversity does not reflect cultural patterns, but is the result of uncoordinated and piece-meal legislation. For example, where medical secrecy is

left to common law (e.g. UK), there is a consensus that the general principles of confidentiality, privacy and ownership do not adequately protect *patients* (Brazier 1992:67). There is a genuine need to harmonise legislation if movement of medical records is to be sanctioned by *clinicians* and *patients*.

The ease of manipulation of digital information, and the speed with which the processing can be undertaken and developed are hostile to our present legal system. Discs containing information may be copied in seconds, the result being identical to the original. The huge legal battles in the USA involving software companies and the uncertainty in the computer industry about ownership and copyright are evidence of this. There are some legal principles that apply particularly to health records; some are new and others are well established. All have considerable difficulties with application to electronic documents.

Confidentiality

Confidentiality is a legal principle, protected by legislation and common law. Yet this principle is not at all clear when considering the movement of information among professionals caring for a *patient*. It is a particular problem as "there is virtually no delimitation of the circumstances in which a donor of information can specify that he gives it in confidence" (Pearce 1988). While legislation through professional secrecy laws (most EC countries) or professional codes (the UK and Ireland) restrict the ability to reveal information, the network of multidisciplinary contacts, all of whom may have a legitimate reason (or duty) to pass on information, may lead to wide propagation of personal health information. It is also clear that the legal process is not attractive to a complainant who is keen to restrict information about themselves. The primary prevention of breaking confidence is far more important than the secondary laws to compensate the victim.

Disclosure, restrictions to secrecy

The legal phrase, "qualified privilege", describes the protection from libel or defamation for people who have a duty to pass information on to others who have a duty to receive it (Pearce 1988:4). This covers doctors or nurses who may be involved in a case conference, making a referral, or giving a reference. Pearce states:

> "Qualified privilege already provides a successful compromise between the right of the individual not to be defamed and the freedom of those who need to pass on information and judgements to do so without fear or liability. The requirements of no malice and dissemination carefully restricted to those with a duty or interest in receiving the information draw limits of protection where they are needed."

Qualified privilege is a principle fundamental to good practice; communication with other health professionals. In terms of the Commission of European Communities directive it can be seen as the professional application of protecting the vital interest of the *patient,* implied or expressed consent, public safety and equivalent rights of others. It is usually a mixture of these principles but may be the exercise of a single one.

Most countries have legislation covering such disclosure to non-health professionals including legal professionals, and *clinician*'s professional bodies have codes of conduct. A summary of the legal situation can be seen in the Appendix.

Ownership and copyright

The control of the movement and processing of medical records is important to protect *patients* and *clinicians*. These two important principles have already been applied to electronic products such as software. Though not usually formerly resolved in the past except in common law, the principles have been well understood in relation to paper records (Pearce 1988:2-3, Kennedy 1989:540).

Copyright	originator of a document has copyright in the expression of ideas or information in that form.
Ownership	principle usually applies to the physical medium containing the information, such as the book or floppy disk.

The writer of a document (or the employer of the writer if the writing is done as part of the writer's employment) has copyright for the content of the document. The owner of the paper, or the recipient of the letter or report has ownership of the document. The holder of a document may pass on information if he owns it and transfers it. He may only copy it if the copy is sufficiently dissimilar from the original. Reproducing the information in the document is not possible while the copyright resides in another.

An EHCR substantially confuses this situation. As a recipient it is impossible to distinguish a transfer from a copy. If digital transfer is the norm then all parties with a copy can claim to own it, as they own the 'medium' on which it is stored. No doubt the copyright, as with computer software, will become the overwhelming issue.

Liability and Accountability

Liability is being bound by or responsible for conformance to specific standards. Not to adhere to such standards invites a potential claim for civil or criminal negligence. It is necessary for the EHCR to specify the accountability of the *clinician*. With the incorporation of technology into the record, there is a need to add liability for the system itself which 'delivers' the record and for its processing. In the case of system failure with harm resulting to a *patient*, or data accessed without authorisation, the *controller* will be liable. This is a principle of the Commission of European Communities directive (CEC 1992:33). Processing data without consent will involve liability, as will failure to fulfil the other responsibilities of *controller* as specified in future legislation. At present *patients* are to some extent protected by litigation in common law (Dick 1991:157). There is an increasing recognition of the potential for liability of designers and operators of decision support systems (Dusserre 1992).

The *responsible clinician*, the only category of person entitled to make an entry in the health care record, must remain accountable both for the quality of that record as well as the care that has been documented.

Identification

Within an Information system, it is important that individuals are clearly identified. There are normalisation processes underway in the EC to establish the dataset for identifying a *clinician*; these may be found in CEN TC251, work items 6.4 and 6.8 (De Moor 1993:11). Apart from the data set there is the concept of 'authentication' (Robinson 1992:1556) and the development of 'digital signatures'. Since 1991 there have been proposed standards for digital signatures released by the National Institute of Standards and Technology (USA), and the Ontario Hospital management (Canada) have, through regulation, introduced the concept of a digital signatures. The need to authenticate a recording by a *clinician* is real, but has not yet been resolved technically.

Legality

In Europe there is no known expression of illegality of the computerised health record. Certain functions such as writing prescriptions by computer may also be illegal[5]. The detailed state hospital licensure laws in the United States vary in their explicit permission to use computers for health records (Dick 1991:758).

Durability

Medical records are required for future purposes, and may be required to be held for as long as 30 years[6]. If used for research purposes in the United States the records may have to be held for 75 years. The durability of digital storage is not proven, particularly of optical disks (Dick 1991:175). Digital data may be encrypted, and require 'keys' to unlock it. To the degree that the EHCR may require software which has become obsolete, may require hardware that is no longer available, or may have 'keys' which have been forgotten (e.g. pin numbers), then durability is much more of an issue in the present climate of lack of standards.

Processing of personal data

Because an EHCR is held on a computer it can be processed. Processing may be any of the following:

Types of processing	EHCR examples

[5] In the UK prescriptions for 'controlled' drugs must be written in the doctors own hand writing. British National Formulary 1993.
[6] Belgium medical deonotological code, Chapter III, Article 46

collection and recording	Creating a record or recording a progress note
organisation, storage	Summarising storing, and backing up the records
adaptation, or alteration	Amending the record
retrieval, consultation, use	Viewing the record, and using it for any purpose such as teaching a student.
dissemination or otherwise making available, disclosure by transmission	Sending the record, or information contained in the record by reporting or by paper or electronic transfer.
alignment or combination	Merging records from two sites
blocking, erasure or destruction	Erasing the record, or moving the record to another computer, or another site.

Processing is one of the main motivations for computerising it in the first instance. It may mean sending a letter to all *patients* who have a certain condition, or counting attendances and revealing the 'league table' of *patients*. Processing is a new legal concept, the scope of which has been extending over the past 10 years. Since the 1992 directive of the Commission of European Communities (CEC 192:63) it has been defined as "any operation or set of operations which is performed upon personal data" and is summarised in the following table. The concept now extends to include non-automated as well as automated processing.

The directive advises banning of processing of health data and legislation for exceptions. This list of processes are all necessary for a EHCR. It follows then that to ratify the directive, legislation allowing the existence of EHCRs.

Transparency

Transparency is a word coined by information scientists to describe an attribute of systems (Gritzalis 1991). This is a new concept, not unique to the application of IT but most relevant in this field. Transparency involves providing the knowledge and means which enable an authorised user or evaluator to 'see' the entire system. Transparency ensures people are aware of what is in the system. A user should know of and have access to all data to which they are entitled, to all data that is available to them. The highest level user must be aware of and have access to the entire system. Transparency applies to design, implementation and use; it is a combination of documentation and tools offered to the user. A transparent system would through documentation and choices presented to the user reveal all information and data stored in that system, and all operations on that data that were available to that user and any other user. It is in essence the property of an information system which minimises the

risk of illegal practice.

The role of controller

Attendant with the principle of processing of data, is the notion of a duty to ensure that the processing is known and is legal. This is only possible if there is somebody responsible for the processing; every HCF will need to nominate a *controller*. Thus the Commission of European Communities directive (CEC 1992:64) defines a *controller* as "any natural or legal person, public authority, agency or other body who processes personal data or causes it to be processed, and who decides what is the purpose and objective of the processing, which personal data are to be processed, which operations are to be performed upon them and which third parties are to have access to them".

This role is, in essence to ensure that a system and its users maintain transparency, as only others can truly judge if these conditions are being met. The Commission of European Communities directive (CEC 1991:70-1) states that personal data must be:

> "a) processed fairly and lawfully;
>) collected for specified, explicit and legitimate purposes and used in a way compatible with those proposes;
> c) adequate, relevant and not excessive in relation to the purposes for which they are processed;
>) accurate and, where necessary, kept up to date; every step must be taken to ensure that data which are inaccurate or incomplete having regard to the purposes for which they were collected are erased or rectified;
> e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes in view; Member states may lay down appropriate safeguards for personal data stored for historical, statistical or scientific use."

The *controller* is given responsibility for ensuring these conditions apply is therefore accountable for their legal application. Ensuring these responsibilities are met is only legally possible if the system is transparent.

The specific problems which morally acceptable regulation of the EHCR must solve:

Several major areas of moral and legal concern follow from the above discussion:

1. the limits of *patients'* control of the creation, movement and processing of the health record.

. the limits of the control of access to and contents of the health care record by *patient*s and *clinicians* and others.

. the establishment of individual accountability through the EHCR as a physical record of the contact between *clinician* and *patient*, and to avert potential negligent use of the health record.

. the appropriate patterns of security enforcement and organisation. Audit thereof for protection of individual privacy, including professional guidelines for appropriate 'whistle blowing'.

. the creation of educational processes which inform both *patient*s and health professionals about their rights and duties.

6. the role of regulation in the development of the EHCR.

. an analysis of what forms of regulation, legislation and processing may be logically lead to increased risks to *patients* and *clinicians*.

Each of the preceding is the focus of a chapter in the following document.

Summary

There are a number of moral and legal principles which may be used to determine the nature of the dangers outlined in Chapter One. These principles may be long established (e.g. confidentiality) or new (e.g. transparency). Some are difficult to apply (e.g. ownership). They have their basis in ethics, established law or new directives from authoritative bodies (e.g. CEC). These principles may be applied to establish the regulation needed to ensure the privacy and safety of individuals is maintained or enhanced.

Chapter Three.
Control of Creation, Movement and Processing of the Health Care Record by Patients, Clinicians and Others.

The international concern regarding application of IT to personal information is expressed clearly by the Commission of European Communities (CEC 1992:2) as "the degree of danger which the processing of personal data may represent for the rights and freedoms of data subjects". As we can only assume that *patients* will be the best judges in most instances of when their rights and freedoms are in danger, there is a moral responsibility to give them some control over the record. The record is however not entirely for the benefit of the *patient*. A subsidiary role is its function as legal document, which establishes the accountability of the *clinician*. What are the limits of control for the *patient* and the *clinician*?

Creation of the health record

The *patient* must have an absolute right to control creation of an EHCR at a HCF unless they have consented to care at that HCF. On the other hand, if the *patient* or someone on behalf of the *patient* requests care then good practice on the part of the *clinicians* and *non-clinicians* demands, through professional codes, that a medical record be created. Failure to attend a HCF may in itself be a significant act requiring attention. The relationship between clinical treatment and health records is clear. If *patient*s want one they must have the other. Further, *patient*s have no right to be treated without agreeing to medical records necessary for adequate treatment unless the HCF is acting improperly. In the event of a mentally competent *patients* insisting that no record is created at a HCF which is acting legally and with due care, *clinicians* have no duty to treat. They should make a formal record of this fact and reasons for their refusal.

The *patient* does have some rights even having consented to care. The Commission of European Communities directive (CEC 1992:82-3) lists the information required to be given to a data subject when collecting information:

"The purposes of the processing for which the data are intended;
The obligatory or voluntary nature of any reply to the questions to which answers are sought;
The consequences to him if he fails to reply;
The recipients or categories of recipients of the data;
The existence of a right of access to and rectification of the data relating to him; and
the name and address of the *controller* of the file."

Refusal of the *controller* to comply with any of the above, may mean that a *patient* might be considered to have a right to receive care without a duty to provide information to create a record.

Movement of the health record

Transfer of an EHCR is different from a paper record. An identical copy of the record, indistinguishable from the original, can be created and sent. The record may be sent to may sites simultaneously. Movement is an operation on the record, and has at least three attributes to describe it: type, extent and conformance.

The type of operation may be described as move or copy, the extent as complete or partial, and the conformance as conformant or non-conformant. These attributes are described in the table below.

Type		the original record and sending it to the new site.
		the original and sending it to a new site, with destruction of the original. Destruction implies leaving it in an unrecoverable state. This would also apply to backups.
Extent		operation involves the entire original record
		operation does not involve all of the original record.
Conformance		to a HCF which adopts a standard of security and processing controls which are broadly the same.
	-conformant	to a HCF which adopts a standard of security and processing controls which are significantly less stringent or more accessible (or might be perceived to be by the *patient*) than the sender's HCF.

Transferring the complete EHCR

'Move' (as opposed to copy) of a record is a particular event which warrants very careful attention. This is the only situation where an EHCR can be deleted. Deletion of EHCRs must be controlled by law and therefore 'moving' must also involve a legal process. Legal difficulties arise if a *controller* can move the EHCR to another HCF without strict rules on validating error free receipt, acknowledgement of the status of the record and agreement to hold the record in a suitable state for required lengths of time.

The transfer of the EHCR may be to a *health care facility* (HCF) which works to standards which are similar to that of the originator of the record, or to a HCF which has differing standards. A 'move' of this nature poses a potential threat to the *patient* and *clinician*. Such

transfers are non-conformant. Interestingly, transfers to HCFs which are more in line with the Commission of European Communities directive may be thought to be non-conformant by a *clinician*, because *patient* access may be greater than at the sending HCF.

Non-conformant transfers are more likely with international movements. While problems exist with transfers within a country (Robinson 1992:1558) and the EC (Allaërt 1992) there is greater concern (CEC 1992:34) about transfers outside the EC. The essence of the problem is establishing standards which enable conformant transfers to be made with confidence. This demands regulation of security and codes of practice.

As movement is one of the aims of producing a standard EHCR, it is clear that these operations will occur frequently. There is certainly a requirement for *patient*s to have control over movement of the record. The extent of that control is uncertain but should not be total. A *patient* or *next of kin* may be unable to give consent when transfer is clearly in the *patient's* interest. Therefore *clinicians* and *controllers* need to be able to make judgements in such situations. Clearly there should be professional penalty and legal redress if transfer is not sanctioned by the patient.

Partial movement of the record

Transferring part of the medical record must be covered by the same rules as transferring the complete record. There are the special cases. For example, it is normal practice in some specialities, such as orthopaedics, to copy the contact note to the general practitioner. Here the 'contact' record functions as the report or communication between *clinicians*. This must be done with the *patient*'s consent at the time of agreeing care with that HCF, as the information a *patient* may convey to the *clinician* in such circumstances may be different.

The movement of information is a separate issue from the movement of the record. A 'report' in the form of a letter, or electronic message allows movement of information without movement of the record. This is the accepted method of communication at present. Consent for 'reporting' is usually implied by the *patient* accepting the offer of referral to another HCF. The *clinician* and *patient* must decide if the transfer of information is conformant, and if not, the *patient* must give explicit consent. An example of non-conformancy might be when a *clinician* working at a clinic for sexually transmitted disease clinic is to communicate with a *clinician* in primary care. Confidentiality rules in that HCF may be much more stringent than in the latter.

The Good European Health Record specification clearly differentiates between the 'contact' recording (progress note) and a 'report'. The latter has a legal status outside the record and requires transmission apart from the medical record. These 'reports' are not part of the health care record until received by a *responsible clinician*. The contents of such a report should probably still meet the conditions imposed by the Commission of European Communities directive on all information: "adequate, relevant and not excessive in relation to the purposes for which they are [required]". *Patients* generally endorse these criteria. Some doctors now send a copy of a referral letter to *patients* at the time of referral. This should be regarded as good practice.

*Patient*s may only be willing to seek medical care on the basis that there will be no flow of information between HCFs. For whatever reason they may not wish their GP to know about all of their medical problems. The same applies to some information which the *patient* may wish to communicate to the GP but not a referral specialist. To deny this right would be against the best interest of the *patient* and the public. *Patient*s who need medical care might not seek it and they may unknowingly be highly infectious. The *clinician* has some duties in this situation.

> Control of information at referral:
>
> A *patient* with rectal bleeding requested that the referring doctor did not reveal that he was homosexual. He was unwilling to tell the surgeon himself or agree to verbal communication by the doctor. This was unacceptable to the referring *clinician* on the grounds of good practice, and a duty to the surgeon who was going to see him. A referral should be agreed on the basis that the needs of both parties can be resolved. The *clinician* should not be willing to lie, and the safety or ability to offer appropriate care of the *clinician* receiving the referral should not be jeopardised.

Specific legislation should exist[7] to give *patient*s control over reports to *other third parties* who are not involved in the care of the *patient* (e.g. insurance companies, employers etc.).

Circumstances where the *patient* would not control the movement of the EHCR would almost entirely fall into the category of reduced competence (see 3.4). Another *clinician* and *controller* may however agree to transfer a record on the grounds that denying the GP access to a particular EHCR would be potentially harmful to the *patient* or the GP.

Imagine a situation where a *patient* has a disease and is under the care of two *health care facilities* (HCFs) including that of the General Practitioner. The current mechanisms for recording care in a paper record are generally as follows:

#	**Primary HCF**	**Reporting**	**Secondary HCF**
1	Record of health care Reports from secondary HCF	via Mail	Record of health care Reports from primary HCF
2	Record of health care Copy of secondary HCF record of care	via Mail	Record of health care Reports from primary HCF

[7] Access to Medical Reports Act 1988, UK

3	Record of health care	*Patient* held reporting	Record of care
4	of *patient* held record	*Patient* held record of care	

The EHCR allows one or all of these situations to exist at the same time. This fact underlines potential for both abuse and improved patient care. It must be said that *patients* can not have it both ways. If the control of flow of information is restricted on the grounds of privacy, the standards and efficiency of clinical care will suffer.

Control over processing of their record

As we have seen the processing of health care records is a broad concept involving virtually all interactions. We have also demonstrated that the purposes of the health care record can be seen in a very general way if all stake holders are considered. How is the *patient* to have control over the processing of health records? Is it possible to exercise this right as an individual, given the complexity of purpose and processing?

The *controller* - who by definition has control of processing - is expected to notify the *patient* before processing takes place (CEC 1992:29) and ensure that an up to date list of processing functions is available to the *patient* (CEC 1992:30). The only way of establishing that the *controller* has been acting responsibly is if the system is transparent, both to users and to monitors. The Commission of European Communities directive (CEC 1992:81) is clear on transparency of processing. This should be achieved by notification of the *patient* of its purpose, the categories of data involved and the categories of third parties to whom the data are to be disclosed.

How can *patients* establish if a process is in their interests? Take for example the releasing of health care record data to drug companies, or a detailed audit or quality control exercise. There is very little data on the use of routinely collected information in the generation of health statistics. What there is not encouraging (Randall 1991). Research is a good example of this dilemma.

Research by automatic processing

There are two forms of research involving the EHCR. The first involves automatic processing of the records to retrieve data. There is no personal access to individual records and data is aggregated. The second involves access to individual records or to data sets from which a *patient* may be identified. This section deals with research in the former case, the latter being considered in Chapter Four, Section 1.4.

involving automatic processing demands that at some previous time a person entered appropriate data. This person must be qualified (and able) to have added the information to the record, and must have wanted to add the information. These two prerequisites may be frequently overlooked. One of the constraints on the quality of the content of the EHCR is the person who enters it. If that person does not understand or agree with the purpose for which data is recorded then the quality will be impaired. This is particularly relevant when c*linicians* are asked to collect data for epidemiological or organisational purposes or non-medical staff enter clinical data.

Research on medical records should have informed consent as the guiding principle

(Bengtsson 1992). This processing is special in that it asserts the value of the personal data for the public good. Research without consent is only possible if there is no chance of breaching confidentiality. This purpose must then be explicitly expressed to *patients* having notes at that HCF, with the mechanism for getting ethical approval for that research. The design and purpose of the research should be available to *patients*, and the results made available through the HCF.

Confidentiality is a complex principle when considered in the context of processing. Details such as address, not normally considered confidential as an isolated piece of data, may acquire confidentiality restrictions by being associated with a diagnosis. An attendance date/time at a specific clinic may acquire restrictions if the appointment list is available to the processor, thus revealing the name of the *patient*. Similar problems of confidentiality can be the basis for ethical committee refusing approval of research involving such processing.

Finally, Can record linkage between databases kept for different purposes ever give reliable results? Checking by consultation with a set of data subjects is the only means of verification. This obviously requires consent. Simitis (1987) in his seminal article on privacy describes examples of data derived from information kept for other purposes which proved to be spurious. In Sweden, 1000 'fraudulent' housing aid recipients were discovered from accurate data in two sites on linking data. Some were quickly convicted, and it was only after considerable effort by motivated individuals that the true situation emerged. Eventually only one of the people was actually shown to have been acting improperly. This example clearly demonstrates that the conclusions drawn from processing information may not be accurate, despite the accuracy of the base data.

Patient competence in relation to control of movement and processing

The *patient* should consent to movements and processing of the record. At times this may not be possible due to inability to communicate or lack of competence. *Clinicians* and *controller*s will be accountable for decisions taken at such times if consent is not given. Attempts to discuss the situation with a *next of kin* or *carer* who is well known to the *clinician* or *controller* should made, and their views recorded. The conformancy of the transfer must be considered.

The rights of parents to control movement of the records of their children is established as important *carer*s or *next of kin*. Generally speaking, parental control will be considered the same as *patients'* control up to the age of 12 years. *Clinicians* should have the discretion not to transfer or in other ways process the records of adolescents who so wish it, provided that they are considered to be mature enough to give informed consent to treatment and non-movement is considered to be in their best interests.

Judgement of competency should be made on the basis of reduced consciousness, or in line with accepted psychiatric practice. Criteria for the evaluation of competence in this regard should be in line with those generally accepted in society.

There is a moral duty to protect the vulnerable, whether or not they are legally defined. This

may involve particular efforts to educate an individual who appears to be acting against his or her own interests. Finally, it may be justified to force an individual to test their competence in some sort of appeal procedure if this is not successful, and the *clinician* or *controller* is concerned.

While there is no professional or legal consensus within the EC about dealing with such issues of limited autonomy, we believe that the preceding constitute goals towards which member states should strive.

Chapter Four
Control of Access to and Contents of the Health Care Record by Patients, Clinicians and Others

While the movement and processing of health care records are major new areas of legal and ethical interest, the issues of access to and control of record contents have been with us for much longer. In what way have they changed with the introduction of the EHCR? First, it is now possible to have a number of copies of a single health record at different HCFs, giving many more people access to personal information. If this information is incorrect, many more consequences may arise. Second, it is possible to control access to the record in a way that was not possible with the paper record.

There is little (though growing) conformity between European states with regard to *patient* access and control of contents. Evidence suggests that general legal and professional principles of privacy are universally endorsed (see Appendix). Differences concern the degree to which individual rights over control of and access to the record can be qualified for reasons concerning the protection of the public or the individual concerned.

Control of access to the detailed contents of the health care records

Access to the detailed contents of the health care record is a major concern to *patients*[8], both to ensure they are being treated fairly and openly and to protect their privacy. An American physician recently documented the access to a typical inpatient record. This included 6 attending physicians, 12 house offices, 20 nurses, 6 physiotherapists, 3 nutritionists, 2 clinical pharmacologists, 4 hospital finance officers, and 4 chart reviewers. Widespread access is real, continuing and potentially unwelcomed by *patient* and *clinician*. Who should have control, and how should this be implemented? Attempts to empirically define access rights (Gritzalis 1992) are irretrievable bound to local attitudes and prejudices.

We will consider access under the headings of the parties that usually have some access to the record.

Access by the patient

There is increasing international recognition of the importance of *patient* access to medical records. Concerns of doctors about causing harm (Ross 1986) and distress (DHSS 1985), and restricting communication (Anonymous 1983) have continued to be expressed by practising doctors, despite evidence to the contrary (Bernstein 1981, Anderson 1988, Gill 1986, Fisher 1993). It is clear that not all *patients* feel they benefit from such access, though most of those choosing to do so report positively.

[8] Sunday Times UK 10/12/89:B8

The right of *patients'* access to the detailed content of their record is increasingly set in legal statutes (Lobato de Faria 1992). The Commission of European Communities directive (CEC 1992:86-7) is clear about the right to "obtain , on request, at reasonable intervals and without excessive delay or expense, confirmation of the existence of personal data relating to him, communication to him of such data in an intelligible form, an indication of their source, and general information on their use." Member states are able to legislate that the right of access to medical data may be exercised only through a medical practitioner. This right is not available in all countries. In some countries there is only partial access. The UK legislation[9] does not allow access to health care records made before November 1991. In Belgium[10] the *patient* only has access to the "objective data", not the "subjective" or written memory of the *clinician*.

For the purposes of trust and improving access to records, *patients, clinicians* and *controllers* will need to respect the context at the time of recording. As we have already argued, non-conformant legal statutes on *patients'* access may be a major barrier to transfer. Despite more stringent conformance with the Commission of European Communities directive at the receiving HCF, the sender of the record may be unwilling to transfer the record in view of the possibility of *patient* access.

Morally speaking, it is a violation of the autonomy of *patients* to deny them access to their health care record. The principle of transparency, and accuracy are impossible to maintain without *patient* access.

> Patient access to the health care record:
>
> A patient has been refused life insurance ever since being admitted to hospital with an episode of severe vertigo. He now applies again. The clinician decides to discuss the health care record which contains a consultant's opinion that the patient may have multiple sclerosis.
>
> The patient is immensely relieved at this revelation as he had assumed that he had something far worse. As it is now 8 years on and he is perfectly well they together decide this diagnosis is probably inaccurate. The result is that he gets his life insurance!!

This said, *patients* should be denied access to the content of their Record if evidence exists that access will cause serious harm to themselves or others. Such harm should not be thought of subjectively (e .g. in terms of distress) but objectively (e .g. in terms of life-threatening

[9] Access to Health Records Act 1990
[10] Loi relative à la protection de la vie privée à l'égard des traittements de données à caractère personnel 1992.

effects). *Clinicians* who argue for restricted access should be accountable for recording their evidence and reasons, which should largely be based on the principle of *patient* competence. When information has been restricted, *patient* should be informed of this fact. It should be further be made clear to the *patient* who should be contacted if and when the *patient* wishes to challenge this decision.

Clinician's control of patient access:

A *patient* is suffering from a paranoid illness and threatening suicide. She was denied access to a result of a full blood count which shows she is mildly anaemic, on the grounds that the report is stamped ABNORMAL. The *clinician* expected such a result to cause inappropriate concern during such an illness.

The *patient* may be even more agitated having been denied access, and this course of action may not be beneficial in such a case. It is difficult to imagine a situation when the *patient*'s request access can be denied with a positive consequences.

There should be a process of appeal against this clinical decision. *Patients* who have had their request for access refused should be able to activate a formal complaints procedure. Here, the professional judgement not to reveal the record would itself be subject to evaluation and a direction could be given that access be allowed. A review committee for this purpose should include both lay representation and a formal representative of the *patient*.

The moral justification for denying access must not be confused with that of 'breaking bad news gently'. For example, the latter might be justified against the background of exploring with the *patient* their understanding and desire for full and frank information at that point of the consultation. The former should concern circumstances where a *patient* has made their desire for such information quite clear.

Information given to the *clinician* "in confidence" (i.e. should not be shared with the *patient*) should not be entered into the record if the *patient* has access to that record. A *clinician* may have to refuse the receipt of such data or rely on memory. If *patient* access is the rule then communications of this sort should not take place unless the care of the *patient* is not at risk if the information is lost.

Clinicians as *patients* may require special guidelines (Anonymous 1993).

Access by clinicians

It is important to remember that a *clinician* does not have an automatic right to see a

medical record (Jackson 1991). The right of access by *clinicians* to the EHCR is granted by the *patient* requesting care from that *clinician* or agreeing to accept care from another *clinician* by referral in the same HCF. Once a *patient* has consented to a *clinician* making an entry into their record, all *clinicians* involved in the *patient*'s care in that particular HCF should have complete access to it. This is of major importance as we believe the alternatives are unworkable and potentially very dangerous. We do not feel that a *clinician* can accept the responsibility for care and recording care without knowing they have access to the complete record of care. Also, 'confidentiality' of any part of the record cannot be guaranteed with access to other non-administrative parts of the EHCR.

Patient control of access by clinicians:

A *patient* is HIV positive and requests that this information is not available to a class of *clinicians* working at the HCF. What does this mean? Is a *clinician* then liable if they treat the *patient* inappropriately? What further information is then hidden from that group of *clinicians*? The results of HIV tests, the results of stool specimens, the drugs the *patient* is taking, the result of a manteau test? Access to all or any of this information could undermine confidentiality.

If HCFs wish to differentiate between *clinicians*, the only moral and safe alternative is to have separate records with communication via 'reports'.

Patients must know, through a public document and also specifically when they first request care at that centre, which professionals have 'clinical' status in the HCF and consequent access to the EHCR. For example, social workers in primary care usually do not, although they may in hospital. Assuming there is choice of HCF, this should be sufficient. It may be necessary, if the practice in many HCFs is not acceptable to *patients*, to limit the access through regulation. However, *clinicians* at individual HCFs are probably the best judges of who requires access in order to maximise the standard of care.

Access to a limited set of records by clinicians:

Health Visitors (involved in care of the under 5s and sometimes the elderly) in the UK may be given access to the records of children under 5 years of age but be required to consult with another *clinician* regarding adults. Likewise a clinic may function best with the Health Visitor having full access to the records. It is important that the *patients* are aware of the policy.

Access by non-clinicians

Here the *patients* must be in complete control and complete denial of access should be available to *patients*. As *non-clinicians* have no duty to make recordings in the EHCR except in the administrative section, they require no access to the record on grounds of accountability. The reality in practice is that many *non-clinicians* do access medical records. Patients are usually happy for this to take place because it allows the patient immediate access to information. They may look up the results when a *patient* telephones, or check spellings and details in the record when writing a letter. The conditions that apply for *non-clinicians* to access a record must be public and available to the *patients* at the time of record creation. If there is an interaction with the *patient* which initiates access, the *non-clinician* should ask for the *patient's* consent at the time. There is a duty at a HCF to educate the *non-clinicians* to respect confidentiality, and breaching confidence must be unconditional grounds of dismissal.

It can be argued that *patients* could be explicitly informed that their own explicit consent to the creation of a record will provide limited access to *non-clinicians* to certain 'non-sensitive' aspects of their record (Dick 1990). It is not difficult to generate scenarios which demonstrate the inappropriateness of fixed classes of data which are more or less sensitive.

> Access to different categories of data:
>
> A *patient* may argue that they are not concerned about confidentiality with categories of data, for example, immunisations or sports injuries. What if the *patient* has a Hepatitis B vaccination because of risk of sexually transmitted disease and is not involved in health care, or has traumatic testicular atrophy after an injury playing cricket?

We reject categorically the notion of more or less sensitive personal health information on the grounds that it is the *patients* that determine 'sensitivity' and not the information.

Access by researchers

Researchers gaining access to the detailed contents of a *patient*'s record must always be with the consent of the *patient,* the *clinician,* the *controller* and an ethical committee. Relevant professional and or educational qualifications pertaining to access for those who are not involved in *patient*'s clinical care but rather for research purposes must be public. Research data kept in electronic form should be anonymised in a standard way described in Chapter Eight.

Access by technologists

The *technologist* has no duty of care involving active EHCRs except when there are problems involving a live system. All development must be on a dummy medical record system. *Technologists* should not normally have access to the EHCR, although if there are technical problems this will clearly be necessary. Access to the *patient's* records must be in the presence of the *controller* and with the consent of a *clinician*. Test records on the live system which are not included in analysis should be available. *Technologists* will need to be educated in confidentiality rules. The total access time of *technologists* to *patient* records should be logged by the *controller* and reported annually.

Access by students

Clinical *students* will need to learn to record their findings on the live system. The detailed mechanisms and requirements are reported in the "Educational Requirements" produced by the Good European Health Record Project. Access to a *patient's* EHCR should involve personal consent of the *patient*, or be via a *clinician* involved in the care of the *patient*, and who has consent to use the EHCR for teaching. Reports generated by *students* should be anonymised in a standard manner described in Chapter Eight.

Access by legal professionals and other third parties

Copying the EHCR to third parties that have a legal or other legitimate interest in the record should involve written consent by the *patient* and a clear undertaking by that third party to use it for specified purposes. Clearly with a lifelong EHCR it may be appropriate to limit the access to a particular part of the record. This process probably requires clear guidelines and possible legislation protecting the *patient* and *clinician*. The Commission of European Communities directive (CEC 1992) gives guidance on when disclosure of personal information may be made without consent:

- where disclosure is necessary in order to safeguard the data subject's vital interest.
- where the data subject has already been informed that the data are to be or may be disclosed.
- where disclosure is required by legislation making an exception to obligation to inform.
- where the data are disclosed for one of the reasons listed in article 14(1).

Article 14(1) lists national security, defence, criminal proceedings, public safety, paramount economic reason, monitoring procedure, and the equivalent rights of others; these are potential areas of violation of *patient* rights and are discussed in Chapter Nine.

Control of the contents of the health care record

The accuracy of the data held in a health record is the responsibility of the *controller*.

The duty of the *controller* must, for reasons of confidentiality and accountability, be exercised through a *responsible clinician*. Establishing the accuracy should normally involve consultation with the *patient*, but may require consultation with other *clinicians* at times. There is a conflict of interest between accountability and durability on the one hand, and the right of *patients* to control the contents on the other. Generally, this is the case at the moment with paper records. Indelible records are a requirement for accountability. Once entered data should remain, amendments effected by creating a new 'version' of a 'transaction'.

Inaccurate data

In the case of data being inaccurate, control of contents should reside with the *patient.* There is a duty to notify others in receipt of this inaccurate data which can be 'hidden' by creating a new 'version' of the 'transaction'. The sense and meaning of the record must be maintained and the reason for the amendment recorded. If accuracy is disputed by the *controller* or *clinician* the data should be annotated with the *patient's* opinion (CEC 1992:86,BMA 1990:7). The errant data may have been the reason a *clinician* took a certain action in the meantime. The principle of accountability and consequence should take precedence over the absolute control of contents.

Excessive and irrelevant data

The data stored in the EHCR must be adequate, relevant and not excessive in relation to the purposes for which it is collected, which must themselves be specified, explicit and legitimate. A *patient* would then have grounds for requesting the removal of data deemed to be outside these limits. It is likely that social data, such as drinking behaviour or sexual practice, will be the subject of complaint in many such instances.

The *clinician* must make an honest judgement of whether the data is significant for the future care of the *patient*, or for litigation purposes. He or she must not only consider him or herself in this matter, but past and future *clinicians.*

As we have already stated, by accepting the offer of care a *patient* consents to access to their record for the purposes of care. There is implicit consent to the addition of new transactions, as demanded by professional codes of conduct. They may specifically state that certain information not be recorded. The *clinician* may go ahead and make the recording if important for future care or medico-legal reasons, and if the information is accurate. The *patient's* dissent should be noted, and the *patient* informed of their rights.

Private notes made by a clinician

Some *clinicians* may be tempted to make informal notes on *patients* which they maintain separately from the EHCR. This will be difficult to regulate. Such informal notes of c*linicians* about *patients* which they would not wish them to see must be hand-written, and absolutely private. In no circumstances should such notes be entered

on the computer.

Chapter Five
The Moral and Legal Problem of Ensuring Clinical Accountability

Accountability implies that there is a set of standards which should be adhered to. Breaching these standards implies negligence, for which there should be a legal remedy in relation to the harm that is caused. These standards apply to both clinical practice and use of health records. There is therefore an absolute requirement that each 'transaction' within the record is attributed to a *responsible clinician.* The EHCR must be a legally acceptable document (Robinson 1992:1555). It must be admissible as evidence in legal proceedings, as well as authorise the validity of prescriptions and other orders. The *responsible clinician* making a recording must accept that he or she is then accountable for the care given. We shall refer to this as the "principle of consequence". Lastly the EHCR must also demonstrate that data has not been used in a manner that is unlawful or unethical.

To preserve accountability there are events apart from the provision of clinical care which should be recorded in the EHCR. Access to records by *patients* or the reasons for not allowing access are examples. It is important to record the basis for a decision to 'copy' or 'move' an EHCR to another HCF and the consent of *patient* or *next of kin*. These may be brief if the need is obvious, but should be detailed and considered if in doubt. Discussion with experts, *next of kin*, *carer*s etc. when information about the *patients* is divulged, should also be recorded in the EHCR.

Further, the EHCR must allow the *clinician* to express information, ideas and justification for actions fully and without restriction. As stated in the Good European Health Record requirements, the record must allow the *clinician* to demonstrate competence (GEHR 1992). With the advent of the EHCR there are new possibilities and new dangers in the area of accountability of the *clinician*. Maintenance of this principle will demand the co-operation of *controller*s, *administrators* and *technologists*.

Preserving the principle of consequence

The EHCR must document responsibility for the accuracy, consistency and completeness of a 'transaction' or entry. The *responsible clinician* making a recording must be clearly and unambiguously identifiable. This responsibility may be individual or shared, depending on the system of delegated authority which is in place. The data set required to identify a *responsible clinician* will be determined elsewhere[11], though this may be by the registration number of the professional body of registration, and a code for that body. Authentication by electronic signature is likely in the future (Robinson 1992:1556). It is common for people other than the patient to be present at the time of contact. The names or relationships (e.g. mother, brother) should normally form part of the record. The place the patient was seen

[11]CEN TC251 has various working groups on identification and authentication.

may also be important, particularly in General Practice.

The EHCR must be able to be admitted as evidence in court when a party is involved in litigation. The principle of identification must be upheld. Likewise, there is a duty on the designer of the system to allow the *clinician* to express adequately the observations made at the time; it must allow the *clinician* to demonstrate competence. The EHCR must be durable, and the system interpreting the EHCR must be accurate and safe.

While the record is a repository for evidence of communication, it is not a means of communication except for continuing care. There is a duty to communicate by means other than the record, by 'reports'. Thus a report issued by a laboratory could not enter the record without a *responsible clinician* making the entry, and a referral to another *clinician* must involve a report or a record that this referral was made by a particular means (personally or via telephone).

With the digital record, which is not inherently sequential, it must be possible to reconstruct the EHCR historically. The contents of the record at any given date and time must be clear and unambiguous. This requires date and time stamps for all 'transactions' and amendments, and dates and times when records from another HCF were merged.

There are particular problems with the transfer of records, which may or may not have been amended at different sites. The Good European Health Record specification (GEHR 1993) introduces the concept of 'transactions', with 'versions'. This allows the possibility of a single record being maintained on different sites with possible amendments at these sites, and subsequent merging of the record. The ethical and legal demand is for a single logical record of care, with no ambiguity about the recording made at a particular contact.

Summarising contact entries

There is concern even in the lay press[12] that no official guidelines have been developed on a suitable summarising methodology for medical records. This is a particular problem with the switch to the EHCR from paper records. For medico-legal reasons the paper record should be retained, since quality of care also demands access to past records. Guidelines developed in our working group suggested a brief record of a 'contact transaction' (or progress note) might contain at least:

- the reason for the encounter;
- the nature of the complaint or problem;
- the most recent accepted diagnosis;
- the most recent treatment plan; and
- the *patient*'s understanding of condition, prognosis and treatment plan.

[12] Sunday Observer, UK 21/5/89

The Good European Health Record specification also contains new transaction types defined in the glossary. The necessary conditions for the successful completion of other types of transaction such as. trigger, continuing care, summary, report or nota bene should be similarly articulated (GEHR 1993).

Recording consent

Patients who have been entered into research trials should have this noted in their record, and depending on the nature of the trial should be in an appropriate part of the record (Contact, Nota Bene or Continuing Care). The details of approval by the appropriate Research Ethics Committee should also be added. Where details might be vital to a future *clinician*, a summary of the research protocol should be included in the record.

Negligent use of the record

Negligent use of the record is related to negligent clinical practice in so far as the record is part of good clinical practice. *Clinicians*, *technologists*, *non-clinicians*, and others may be motivated to falsify an entry in a health care record, or may through incompetence or lack of knowledge make inappropriate recordings. It is widely recognised in the literature on security that the major threats to systems are from insiders, people working within the organisation. Next we will consider some of the possible abuses available to *clinicians* or others working in the organisation.

Altering records

Clinicians have in the past altered or destroyed the contents of records. The temptation to alter may be substantial if the risk of detection is small. The nature of information stored on digital media makes detection very difficult. Medical insurance companies warn against this temptation (Hawkins 1985:174). The solution must involve *technologists*. If the system is built in such a way that the storage of data is sequential with complex checks on completeness and other indices it may be 'impossible' to retrospectively change data without detection. But, any ability to destroy past records is unacceptable to most *clinicians*. A EHCR should therefore be written on indelible media, or if this is not feasible at present the architecture should be designed in a way that is conducive to this requirement.

Falsifying records

Date/Time

Whether or not records are indelible, it will be possible to falsify records by entering a false Date/Time in a computer clock for example. This must not be possible. It may be possible for a system to remember the last date/time used in encrypted form and never allow the recording date to be prior to this.

A new indelible record with alterations

Even if records are stored on indelible media, such records may be copied onto magnetic media where it may be altered. The records may then be copied as a set onto a replacement indelible storage device. The ability to alter medical records by *patients* and *clinicians* (with help from *technologists*) will probably always remain. The only protection would appear to be maintenance a copy of the record by *clinician* and *patient*.

Inaccurate recordings

Although aware of certain risks, a *clinician* may defensively omit recording important details or falsify them. Continuing access to the record by *patients* is the only way to establish accuracy.

Falsifying identity

Entries may be made by users or *technologists* who use another's access code.

Inaccurate or insufficient records

This problem is an old one and is not peculiar to the EHCR (Hawkins 1985). However, it is possible, in an EHCR, to prompt for particular information. *Clinicians* may feel that this is restricting their clinical freedom, but some warning message, data entry checking or validation rules may be instituted as part of an EHCR system.

Non-objective records

The use of phrases such as 'malingerer', 'bloody nuisance', or 'promiscuous' in records cause problems as they are open to wide interpretation and may stigmatise the *patient* personally or in the eyes of future *clinicians*. It of general concern[13]. The only protection from this sort of recording is *patient* access.

Summary

Preserving consequence and accountability is important to protect *patients'* rights. It requires technical solutions and codes of practice for health professionals and *technologists*. Access by *patients* and ultimately a *patient* held copy of the EHCR are the best mechanisms for restricting negligent use of the record. The ability of *patients* to monitor negligent use of EHCRs will depend on their knowledge of their rights and the ethical and legal framework in place. Education is therefore a fundamental requirement.

[13] Sunday Observer UK 24/12/89

Chapter Six
The Security of Electronic Health Care Records

"No security can be achieved if everybody is hostile and all machines are faulty." (Pfitzman 1992)

Security, according to the Oxford dictionary, is "safety against attack, impregnable, reliable, certain not to fail, in safe keeping, and firmly fastened". All of these concepts are valid when considering the EHCR. There is an evolving framework, both theoretical and legal, to ensure and maximise the security of information systems. Security of systems is generally classified as follows:

- **Confidentiality**, ensuring people can only access authorised information;
- **Integrity**, ensuring systems do what is expected of them; and
- **Availability**, ensuring that systems are available when required.

Security is not just a technical issue, but includes physical security, procedural security and staffing security (Barber 1991). There is a generally accepted need to standardise the security policies and mechanisms for achieving them at an HCF.

Security is a major concern for all involved in the implementation of information technology (IT), particularly those in banking (Sherizen 1991) and health care (Barber 1991). Security is usually considered separately from the information system itself (Baskerville 1988), but in fact it has no separate role. Research efforts to integrate privacy into the data model have been published (Biskup 1990). There is a growing literature and expertise in the field and AIM projects such as SEISMED are tackling this problem specifically.

Security is usually expressed in terms of the threats and mechanisms for avoidance, mitigation and control. It is not commonly expressed in terms of duties, and consequently it is difficult to be sure who is responsible. We shall consider security in terms of the duties of individuals and propose guidelines for debate. Security requirements for HCFs should be expressed in such terms to motivate individuals involved in EHCR developments.

The duty of administrators

Administrators are responsible for the physical safety of the system and data, and the software that runs it. Theft of information, software, and even computer facilities occur (Audit Commission 1990). Power failure is a further threat to availability and data integrity. There are now sophisticated processes to go through to evaluate security of information systems (Barber 1992) and adequate security policies are essential. These measures are however not attractive on the whole to owners of information systems as the cost benefit of such undertakings and the necessarily guess work involved (Baskerville 1988:157) are not attractive. Unfortunately motivation is usually very low until a problem occurs.

There is a tendency to think of technical security as the total answer (Barber 1992:349). But technological advances may aggravate problems due to greater interdependency, greater complexity, more dangerous problems being tackled, no legal responsibility for system faults, and attackers having more powerful tools (Pfitzmann 1992:371).

Good practice of the controller

The *administrator*, who may be the owner of the system, is responsible for nominating a *controller* for the system containing EHCRs. The good practice of the *controller* may be by self regulation of a profession, or the duty of the *administrator*. Providing the physical, hardware, software and educational resources to the *controller* must be the duty of the *administrator*.

Education

Providing educational resources is a duty of the *administrator*. Acceptance of a EHCR may require substantial educational efforts (Dick 1990:139) and new users will need education in safe use of the system, as well as moral and legal issues. Resources for education must be costed as part of the system, and deemed adequate from a security point of view. The EHCR itself may have a significant role in the education of *clinicians* (GEHR 1993a), a use that will require special administrative arrangements.

Protection from outsiders

There are 'outsiders' who will attempt to 'hack' into systems. This is usually only possible when a system is connected to the outside world by a modem, or within a large establishment. Branscomb (1991) has stated:

> "The privatisation and commercialisation of information do not sit well with computer hackers, who look on computer networks as an open sharing society in which the skilled contribute to the welfare of the co-operative. Yet, like pioneers on the Western Frontier, they are confronted by those who wish to fence in their private domains."

The technology available to hackers is now substantial, but systems have many more safety features to prevent hacking. The *administrator* must be aware of these risks and ensure that adequate precautions are taken to prevent 'attack'.

Security policy

Providing an explicit security policy (Pfleeger 1991:516) is the duty of the *administrator*. The security policy should indicate clear security goals of the HCF, who will be responsible for achieving them, and what resources will be available. The auditing of security should also be documented. This policy must be acceptable to the *controller*. There is a duty to protect the system from physical damage, from outsiders (whether or not they are authorised), and to ensure that the mechanisms for transfer of EHCRs are confidential.

Availability

Paper records depend on having them physically in front of you. The EHCR depends on power supply, cabling, many local and distant hardwares (including printers and displays) and software. All of these have failure rates, though these are rarely quantified. The development process has economic ramifications of a different order than paper records; new software requires new hardware. Problems that arise require knowledge that is not required for employment in *health care facilities*. Barber states (Barber 1991):

> "Systems are routinely used by staff who expect them to work, and trust their responses, and who do not know how the job was handled without computers. Furthermore, current staffing levels frequently preclude the rapid return to the previous manual systems."

As the motivation for implementing an EHCR is at least partly financial, this situation is likely to be a feature of such implementations. The responsibility is then to avoid system failures and 'downtime' and have backup systems and power supplies as defined in a security policy. This investment should be part of the system cost.

There is a duty to ascertain a system's downtime at other sites and ability to restore quickly when buying a system. *Administrators* should include performance standards, guarantees of reliability and on going maintenance in the lease. There is also a duty to take precautions against sabotage, such as viruses, and to have adequate backup and emergency capability. Legal redress is no protection to users.

Physical safety of the system

The computers running the system, and the backup of data should be made physically safe. The *administrator* must publish the mechanisms for ensuring this in the security policy.

Risk management

The system must be available to the *clinicians* and *patients* and other users. The *administrator* must be aware of the risks to the system, the probability of such events, and the recovery mechanisms if such events take place. While profitability must be considered in such a calculation, there must be pressure to ensure that this is balanced by genuine concern for the rights of *patients* and *clinicians*.

Administrators need to manage the risks of complete failure (Pfitzmann 1992). The best protection is decentralisation and independent operators. The Swedish and Norwegian Medical Association (Bengtsson 1992) see this as a fundamental aspect of security. They have directed that computers should be organised at the "base unit", a hospital department or community health centre.

The risk of software errors need to be estimated, and testing procedures validated.

The duty of controllers.

Good practice of 'insiders' and data accuracy

The duties of *controllers* are extensive and have been described earlier. The security and accuracy of the data, and the 'correctness' of processing are their prime responsibility. *Controllers* can be seen as having the responsibility for the practice of insiders, the greatest threat to security (Dick 1990:173). However, it must be acknowledged that at "times security against insiders cannot be achieved on principle" (Pfitzman 1992:370) and it is important that *controllers* and their superiors are aware of the need to develop trust in the working environment. This will be achieved through education and support of the users. Policies against sharing access mechanisms (e.g. passwords) and respecting confidentiality must involve grounds for discipline or dismissal. Staff should sign agreements that prohibit these practices at the time of employment (Dick 1990:172).

Accuracy of information is also the duty of the *controller*. Again the users will have to be able and willing to enter data accurately, and mechanisms for *patients* to check accuracy must be established. The *controller* must also be sure that the security policy meets legal requirements and is being maintained.

Data security

Controllers have the primary responsibility for data security. Bakker (in CEC 1991:191-3) gives a summary of the potential threats to "data integrity and usage integrity". He classifies the threats as due to the hardware or software. He is concerned about the security and safety issues, particularly those arising from the freedoms brought by the movement to the PC environment and networking. Theft of "data carriers" now may involve floppy disks, or small machines. Downloading data from a hospital information system to a PC may allow interrogation by extremely sophisticated PC software. Logging on to a hospital information system via a PC may allow sophisticated routines to determine password and there are the special problems of smart cards.

Monitoring the movement of records

The *controller* must establish that records are only transferred with the *patient's* and *clinician's* consent, that the HCF requesting the record is authorised to do so, and that the communication is safe in terms of errors and confidentiality. Only the necessary information (parts of the EHCR) should be transferred.

The lack of legal harmonisation in Europe will make the insurance of conformant transfers quite difficult, but the *controller* and *clinician* will take joint responsibility for this unless the *patient* gives unconditional consent. Requests for *patient* access must be individually considered in light of non-conformancy. Resolution of this problem will require expensive debate, but is urgent if record transfers are to proceed.

The duty of users

Users must respect the confidentiality of *patients* and *clinicians*. This duty is established in common law. Failure to do so will result in dismissal. We have already recognised the profound effects such breaches of confidence can have, and the reluctance of *patients* to take legal action as more publicity will result. Prevention of breach of confidence must be the aim.

Users have a duty to ensure that they are reasonably trained to use a system before they attempt to do so. This must be made possible by adequate education, and information from the *controller* and *administrator*.

Users have a duty to ensure that they enter accurate data. The normal mechanism should be to check with the provider of the data at the time of entry.

Fraud in information systems (Audit Commission 1990) is usually through unauthorised alteration of input, alteration of computerised data, alteration or misuse of programs, destruction, suppression or misappropriation of output. Users have a duty to be honest and avoid such practices, and to inform the *controller* or *administrator* if another user behaves immorally. Such reporting should be confidential and capable of being made anonymously if the critic so wishes.

Many facilities, such as query languages, open systems, and fourth generation languages give access to data and software development to people without formal informatics training. It must be clear to users that they have a duty to obey all legal and moral restrictions on the processing of health information.

The duty of technologists.

an EHCR will mean for the first time that the health record will only be available to health staff (clinical and non-clinical) with the assistance of *technologists*. There is an increasing recognition that such technological developments within the health care domain have implications for the ethical education of *technologists* (McFarland 1991).

It is important that a system does what it was designed to do and that it always does it. This is called system integrity. Software safety is a burgeoning field, with a long history in space exploration and defence. Clinical systems, whether they involve an EHCR or not, demand stringent safety evaluation.

Bad practice and operation

Abuse of personal health information will be particularly easy for *technologists*. It is important that they are educated about the importance and benefits of confidentiality, and have a mechanism for expressing concern and resolving problems without placing their employment at risk (McFarland 1990).

Technologists have a duty to maintain and debug the software, and to test the revision (Dick 1990).

Technologists have a duty not to access data or computer facilities in an unauthorised manner, or to sabotage of facilities. They have a duty not to intentionally or unintentionally infect a system with viruses and other computer sabotage (Dick 1991:173)

System design

Designer motivation

The motivation of designers to provide efficient, safe and transparent systems for EHCRs must be high and sustained. Abuse at the design stage could cause immense problems. A designer's 'ego' may become intertwined with the system she or he is designing, thus becoming threatened by changes to the system. Designers have a duty to ensure that their practices are thorough and appropriately motivated.

Appropriate methodologies

Designers have a duty to use appropriate technologies for a task. Design and implementation may be overly simplified in an effort to proceed quickly and with apparent efficiently. Security should be an integral part of the system design, and with requirements and evaluation criteria having the same status as other facets of the system. Encryption techniques should be robust and standard.

Appropriate technology

Security must not be seen as a purely technological problem, and designers need to ensure that the managerial aspects are specified in addition to the technical aspects. It is tempting to use technology to provide control over the movement of EHCRs, but *clinicians* and *patients* have control at present and this may be most appropriate.

Unrealistic expectations

Technologists must also expect users to behave in unpredictable and irresponsible ways. There is a moral duty to build security requirements into the system if performance and the practice of the user is not overly disturbed. The use of personal computers and growing access of non-technical people to data manipulation techniques (through Advanced PC applications and 4GLs) means that simple access control is insufficient (CEC 1991:191-3).

The duty of Third parties

Third parties must respect the confidentiality of data even if anonymous. The confidentiality of the HCF or *clinician* providing the data must also be respected. The third parties must have consent to access the data. The purpose for which the access is allowed and the time

frame must be explicit. Third parties must have ethical approval for access to the data. They also have a duty to ensure that the data is accurate.

Processing undertaken by the third party should not threaten confidentiality of any party, and should be declared as the basis for access, preferably in a contract. The processing should also be validated, and the results checked with the HCF supplying the data before action is taken.

The duty of the State

The role of the state must be as an ally to the parties involved in health care. As an ally of *patients* the state may pass restrictive legislation protecting privacy, or enable litigation for damage. As an ally of *third parties* the state may dictate that access is given to statistical offices for the purposes of health policy development. Through professional organisations *clinicians* are likely to press for their interests to be met.

Legislation

Legislation as a means of regulation is likely in this developing field. It is one of the most powerful means of bringing a situation to the attention of health care managers. There are a number of areas where legislation is particularly necessary.

Computer crime laws

Computer crime laws are now legislated in most countries (Baskerville 1988:167). These are designed to deter unauthorised access. Machines and storage devices are becoming much smaller. A machine that is extremely powerful with huge storage may be smaller than a PC. These machines are also expensive and in small HCFs the ability to prevent theft may be limited. There may be a need in law to differentiate between theft of a home computer and a computer used to store EHCRs. As new technology becomes available legislation may need to be extended.

Privacy laws

Privacy laws may need a major overhaul in an 'information society' (Simitis 1987), and not just in the health care domain (Turn 1990). The principle problem is that *patients* have no redress for breaches of confidence without further threat to privacy. The Data Protection registrar in the UK has made it clear that this issue is one for parliament to address[14], while reporting concern at the present situation. Baskerville (1988) predicts "intervention can be expected to grow tremendously in the future".

Managerial motivation

Motivation of *administrators* is necessary for successful implementation of the EHCR. This motivation must overcome the resistance to the introduction of computer systems and ensure

[14] British Journal of Health Care Computing 1993;10(8):10

adequate security. Despite the data protection act in the UK, one commentator has stated that "it must be doubted whether many NHS systems would pass even a cursory data-protection audit." (Barber 1991:345) Two health establishments were prosecuted in 1992 in the UK, probably indicating how few were investigated. A*dministrators* may as yet be unaware of the role of IT in health care, or may be very reluctant to become dependant on it. Poor security is certainly an immense problem for management, and the only way to improve the uptake may be to ensure that security is implemented to a level appropriate for that institution. Standards and legislation are necessary. Accountability for breaches of security should be clear.

Certification of software

Commentators in Europe are concerned at the lack of standardisation in software for EHCR implementations (Christensen 1992:390). Standardisation of software safety testing procedures should be developed.

Education

We have argued throughout this document that education is a fundamental requirement for a morally acceptable implementation of the EHCR. This places a duty on the state to assist in the development of education programmes. We will argue in Chapter Seven that *controllers* may require formal education and become a profession of their own.

External evaluation and regulation

The Commission of European Communities (CEC 1992:37) directs that member states designate one or more independent supervisory authorities. These must offer specific regulation of HCFs, and allow individuals to report bad practice anonymously. This body should have its own specific responsibilities (e .g. to introduce alterations to security regulations in the light of technological advances and to monitor security procedures in a regular manner). It should also have specified powers (e .g. the right to investigate purported breaches of security, to communicate directly with regulatory bodies which are external to the HCF). A designated officer of this authority should have access to all EHCRs for the purpose of auditing good security practice. The procedures by which designation occurs must be clarified.

Establishment of an independent authority will allow development of protocols and guidelines without state legislation if necessary. Barber (1990) has pointed out that "the department of Health had failed even to deliver a promised voluntary code to protect the confidentiality of patient records, arguing that common law did so adequately". Offering a way forward for *administrators, clinicians* and *technologists* in such a situation is extremely difficult.

Summary

There has been a major effort to standardise the evaluation criteria for information systems

security in the EC. The result is the ITSEC (ITSEC 1991) document which offers a methodology for describing and evaluating systems (or 'targets of evaluation') to six different levels. This methodology should be accepted by developers of health care systems. Security needs to be expressed in terms of duties to ensure accountability.

Chapter Seven
The Moral Importance of Education in the Implementation of a good European Health Care Record.

It is clear that abuse can not be controlled by security. A *responsible clinician* will always be able to break confidence for example. It is also clear that abuse of health care records is not a major problem at the moment. This is largely due to the moral education of people currently working with health care records.

The need for staff education is well established. Lack of education and training has been blamed for the collapse of early IT projects, and data protection increases the education demands substantially (CEC 1991:14). Education must be ongoing, and appropriate to the role of the person. Nobody is protected from this requirement. *Technologists*, especially those involved in development, *administrators*, *non-clinicians*, legal professionals, *clinicians* and *patients* all require information to adequately deal with EHCRs and understand the rights and duties involved.

Most aspects of security and bad practice outlined in the preceding chapters require education in order for regulation to succeed. The need for education extends to all parties. There is also a general need for the community to understand the issues and be part of the general education curriculum.

requirements:

Who	**What aspect**	**When**	**By whom**
Patient	Rights as data subject	When a record is created	*Controller*
	Right of access	General	Society
	Right to control access	When record created	*Controller*
	Right to control movement	General	Society
	Right to control process	When record created When new process	Society
Clinician	Duty to *patient*	General	Profession & *Controller*
	Duty to *controller*	When employed	*Controller*
	Accountability	General	Profession
	Avoid bad practice	General When new system	Profession & *Controller*
	Use a system safely	New system Employed	*Administrator*
Controller	Duty to *patient*	Employed New system	Society or profession
	Duty to *clinicians*	Employed New system	Society or profession
	Legal responsibilities	Employed New system	Society or profession
	Maintain transparency	Employed New system	*Administrator*
Admin	Duty to *controller*	Security policy	*Controller*
	Duty to users	System installation	*Technologists*

Without a program of education for *patients* and *clinicians* concerning all of the topics of the preceding chapters, regulatory policies will inevitably be unsuccessful. The key components of such a program concern curriculum design and the identification of specific target groups requiring particular education. *Controllers* have the most pressing need as many of the incumbent duties are new and untested.

Who will be responsible for this education? The responsibility for a HCF's records will be with the *controller*, as will the educational requirements of staff members. There may be a

designated officers in each HCF accountable to the *controller* , and working closely with those with responsibility for security. The education of a *controller* will be complex and require considerable familiarity with both theory and the work environment. Given the complex requirements and the threats if errors occur, the education of the *controller* must be the responsibility of the state or through development of a new profession. This may be the only way of being sure that standards are met. This may be delegated to appropriate educational establishments. *Administrators* must be responsible for the *controller* being adequately trained, and that sufficient educational resources are available to all staff. Thus education should be part of contractual commitment to follow agreed regulatory policies.

Summary

Education is a fundamental requirement for the legal and moral implementation of EHCR systems. The education of *controllers* is a high priority, perhaps leading to the development of a professional body. The state and *administrators* have a duty to provide resources for education, and curricula need to be agreed.

Chapter Eight
Regulation of the EHCR

Soon after the implementation of information systems it became clear that they may constitute a great threat to individual privacy. Several countries moved quickly to enact specific laws. The privacy act of 1974 in the USA was general in intent, but recognised the threat of computer systems. The first specific legislation was in a part of the Federal Republic of Germany in 1977, the "Bundesdatenschutzgesetz" (Biskup 1988:575). Concerned individuals and pressure groups have continually argued for improved legislation, while users have demanded technological solutions. The result in the USA is that privacy of *patient* records is " governed by a crazy quilt of statutory, regulatory and common-law rules and is often inadequately protected." (Dick 1990:164). It is important that Europe attempts to regulate the EHCR in a co-ordinated and careful manner, so that the aim of facilitating movement of the record is realised.

A Strategy for Regulation

We have argued that there is a prima facie argument for regulation of the EHCR. Such regulation will evolve as the concerns of *patients, clinicians* and others are expressed and experience of the EHCR grows. There are two initial stages in a strategy to regulate the EHCR. The first is to establish, as a common denominator, the security and operational requirements for an EHCR system allowing transfer of the record. The second is to adopt measures that will regulate the use and transfer of the EHCR in a way that maximises the benefit to *patients, clinicians* and society.

First stage

What is the lowest common denominator concerning legal and professional responsibilities, in design, use and transfer of the EHCR? Conformancy of transfers would seem to be the biggest barrier to transfer in practice. The literature suggests this can only be achieved with consistent international rights of *patient* access, and access to third parties. Consider the access of third parties. Denmark allows private individuals and public authorities to pass on data when required for carrying out a scientific or statistical investigation of paramount importance to society at large (Lobato de Faria 1992:363). France does not allow this in principle. There may or may not be common ground in these views. Providing aggregated data with the smallest identifiable group of *patients* being greater than 1000, for example, may be acceptable to the French. The Danish may come to recognise the risks of their policy. In the meantime, transfers of records from France to Denmark could not be considered conformant and the *patient* would need to give informed consent.

This first stage must focus on a strategy for integrating already existing legal and professional regulation as much as is possible with minimal moral constraints. It must involve groups representing *patients, clinicians, non-clinicians, controllers, technologists, administrators* and *legal professionals.*

Second stage

The second stage involves a mixture of legislation, development of codes of conduct, and regulatory bodies. The overall aim should be harmonisation to allow movement of records, and the incorporation of security and education into system specification, costing and resourcing. Ideal regulations should be developed, towards which the Community should evolve as a whole. In the long term, this ideal should be compatible with a plurality of computerised records, analogous electronically with existing circumstances, and with a personal computerised record or Medical Record Card.

Codes of conduct

Codes of conduct are proposed by the Commission of European Communities directive (CEC 1992:36). There are examples already in countries outside the EC (Bengtsson 1992, RACGP 1993). While recognising the variation within a professional group they propose certain features:

"They are drawn up voluntarily by a profession or trade, although they may be encouraged by the authorities;

they apply or fill out the legislation applicable, but they must remain within it; and

they are not binding on third parties, or on the courts, which may always give priority to their own interpretation of the legislation."

Codes of conduct are essential for *controllers, clinicians, technologists* and *administrators*. Legislation may be derived from such codes as EC countries have made them binding in the past (CEC 1992:37). Codes of conduct must address security and education as well as good practice. The management techniques appropriate for a HCF must be addressed.

Regulatory bodies

The Commission of European Communities directive (CEC 1992:37) states that "each Member State shall designate an independent public authority to supervise the protection of personal data". Regulatory bodies may have to be decentralised and have a specific focus, such as health care. They should be empowered to ensure that legislation is being adhered to and establish that it is reasonable and functions appropriately. They should negotiate with bodies developing professional codes of practice, and with legislators. They must ensure that education is adequate.

Legislation

The Commission of European Communities directive (CEC 1992) is an adequate basis for legislation in the domain for the present. If movement of medical records is a basic aim, then harmonisation within the EC must be a priority. The operation of moving a medical record (i.e. copy and delete) must be a priority for establishing a legal process. Doing so will require a number of conditions which will require legal definition.

Privacy and security issues will be the focus of legislation, to ensure protection of *patient* autonomy and confidentiality of systems.

Specific codes required

There are some specific operations which warrant early attention as they are required in many fields.

Standard methodology for anonymisation

There must be a standard process for anonymising personal health information. The risk of identification must be established. For example, in a practice of 5000 *patients* in London[15] the following data items were found to be unique at the following percentages:

Data item	**Percentage patients with unique value**	**Percentage patients who share value with less than 10 others**
of birth	%	%
registered with doctor	%	%
	%	%

Are these data items anonymous? They are clearly not if associated with other information, and as other lists may be available, clear guidelines on this aspect of anonymising data are necessary.

The use of EHCRs by students demands anonymising of records. We have a proposal for anonymising of detailed datasets.

- No demographic variables occur at a frequency of less than 100
- No access to any public list that could reduce the frequency of the demographic list by further processing.
- No access is given to people processing the data to confidential lists containing such data.
- That all dates in a dataset are altered by a set amount to make the date of birth the 1st of January. This will maintain the relationship between events and age in neonates.

or

- That all dates in a dataset are altered by a set amount to make the date of admission or start of episode the 1st of January. This will maintain the relationship between events and an episode of care. The day of birth should be altered to the 1st of January. This will allow comparisons of episodes.
- The names of *clinicians* should be removed but their profession maintained.
- The HCF name should be removed.

All dates that are not altered may allow combination with other data (such as admission lists) and so reveal the *patient* identity.

Security and management policies

[15] Personal communication S. Heard

Adoption of security evaluation standards such as the Information technology security evaluation criteria (ITSEC 1991) is imperative. This is only of value if there is an appropriate framework for security requirements (Pfleeger 1991) and the security aspects are part of the system (Baskerville 1988, Biskup 1988). There is a potential problem with the motivation of managers in this area, and with litigation slow to proceed, pressure to formulate codes of practice and possible legislation will be required.

Processing

French law has led European legal developments by specifically declaring that "No judicial, government or private decision involving a finding or judgement on human conduct may be based solely on automatic processing of data that give a description of the individual's profile or personality" (Turn 1990). This principle is in the directive of the Commission of European Communities on data protection (CEC 1992) Article 16 and is subsumed in the generic principles of objectivity and qualitative evaluation proposed by Gritzalis and Katsikas (1991).

Controlling derivation of data, such as the total cost of individual *patient* care, without their consent will be difficult to control without clear guidelines and legislation. Specific codes for the processing of health data, methods for establishing reasonable accuracy, and appropriate uses of derived data will be necessary.

Summary

Regulation of the EHCR can only proceed if there is an initial harmonisation of laws, and then a progressive adoption of moral and legal regulation across Europe. Specific problems warrant regulatory efforts outside this framework.

Chapter Nine
Slippery slopes and the State

There are a number of "slippery slopes" which must be contemplated. First the type of health care environment we want in the future. Our approach to the record will determine this to some extent. Second the argument about public interest and potential abuse by the state. Third the excessive use of technology in security. Automation will also allow the association of other public functions
with health care and finally the lack of differentiation of roles that may arise in a HCF, leading to poor regulation.

The health record environment

Of major concern is the type of health care record environment which is going to develop with the widespread application of IT and the advent of the EHCR. There are three general models. The first is an electronic version of the present state of affairs; with small HCFs and independent versions of the record with formal communications by reports or hand-held records. This 'closed system' works well if there is a strong attachment of *patients* to the HCFs, and they follow predictable pathways to receive care. The second is large HCFs with a common record. The HCF may eventually be a region, country or the EC itself! This 'open system' will work well if the *patient* attends many different centres in an unpredictable way. It will maximise the ability of *clinicians* to have access to *patient* records even if the *patient* is not attending. Finally, a '*patient*-held system' with *patient* held records, doing away with HCFs for record storage is a third model. This maximises *patients* control and privacy, while minimising the access to the *patients* record by *clinicians* except when the *patient* is present. These models are summarised in the following table:

Open	**Closed**	**P a t i e n t held**
Centralised record storage.	Hospital department, Community Health centre, General Practice or similar hold record.	*Patient* holds record.
Maximum access to *clinicians*.	Maximum control for *clinicians*.	Maximum privacy and control for *patients*.
Maximum threat to confidentiality of *patients* and *clinician*.	Compromise in *patient* care and privacy; suitable if continuity is valued.	Maximum threat to *patient* care as record may not be available.
Dependant on development of telemedicine.	Moderate technological requirements.	Dependant on digital hand held storage. Will require backup?

Maximum access for epidemiology	Maximum access to consistent data (limited recorders)	Maximum access to records for research via patients.

Technical sources (Robinson 1992) tend to argue for the open system or *patient*-held system, while *clinicians* (Bengtsson 1992) tend to argue for the closed system. The ability to maintain a single logical record of care (GEHR 1993) will allow progression in all directions, or duplication.

Open system

The open system is defined by large HCFs involving many sites where health care is offered. It requires major networking and access control. *Clinicians, technologists* and *administrators* may be interested in this model as it allows access to the same record from many sites, while statistical information will be freely available. The control will however be passed largely to the *controller*, the *administrator* and the *technologist*s of the HCFs. Control by *patients* and *clinicians* will always depend on the security of the system and access rules.

> ’Nightmare scenarios’ with an open system:
>
> With an open system, the state will potentially be able to process records without consent for whatever purposes they would wish on the grounds that anonymity was preserved and the purpose of the processing fell within a category in the public list.
>
> A large HCF may be sabotaged or physically damaged, thus destroying all the data on many thousands of *patients*.

One can argue morally that if <u>any</u> transfers of records are envisaged between HCFs that the moral and legal regulations required for an open EHCR system must be in place. Trust, as we have already argued, will continue to be a prerequisite for an EHCR system, and if transfer of records between HCFs are not frequent and require the *patients* consent, a substantial portion of the regulation can be in the form of the threat of litigation.

Closed system

The closed system is a model based on present operations and is therefore easier to understand and makes current regulation more applicable. The EHCR is substantially in the control of *clinicians* who have written it. Processing and access would be at the HCF.

Certain complexities arise in the closed model. There will be many EHCRs each containing a mixture of recordings made at that HCF and reports of care at other HCFs. There may be partial or complete copies of the records of other HCFs forming part of the record. The ability to cope with this situation is critical, maintaining a single logical record. This can be achieved through appropriate labelling of each transaction and the concept of versions outlined in the Good European Health Record specification (GEHR 1993).

The notion of a closed system implies a specific duty to care by the HCFs holding a record for that *patient*. This may well be considered of value by *patients*.

> ’Nightmare scenarios’ with a closed system:
>
> The small HCF operating in a closed EHCR model may stop co-operating with that *patient*, and be unwilling to release the record to other HCFs. Or the HCF may not be available at a time when a *patient* is seriously ill and the *patient*’s care may suffer in consequence.
>
> Internal security may be much less stringent, and theft of computers, for example may be a real risk.

The level of agreement amongst suppliers of EHCR systems will have to be as stringent as in the open model, but will be more difficult to monitor.

Patient-held record system

In this situation, a *patient* would carry a smart card or similar device with them, and offer it at the HCF where they needed health care. The *patient* has control of access and processing as well as ownership. Offering good quality care is however dependant on the *patient* having the record with them when care is required. *Patients* who are not competent may suffer particularly under this system.

> ’Nightmare scenario’ with a patient held EHCR:
>
> A *patient* arrives confused and aggressive at a HCF with an obscure condition which is the cause of the condition. He attends the HCF from time to time but is not known to the staff that night. He will not produce his *patient*-held EHCR. He is thought to be drunk and removed from the premises.

Summary of the EHCR environment

The nightmare scenarios that can arise in the different EHCR environments are due to access to care, access to records and control of records. Access to care is implied within the closed model: if a particular HCF holds the *patient* record and controls it, then they have a duty to provide care. Not to do so would jeopardise the *patient's* health care. This model, if associated with a small HCF (or base unit (Bengtsson 1992)) demands a personal relationship between *clinicians* and *patients*, and assumes predictable movement of the *patients*. Access to records at the time of care, particularly if the *patient* is mobile and telecommunications are problematic, is highest if the record is *patient* held. If the access may not be at the time of care, and the *patients* movements are less widespread, the open system will provide greatest access to records. Processing of the record will be difficult if *patient* held and particularly available in the open model. The open model is of more interest to *technologists* (Robinson 1992) as it fits models common in large business (e.g. airline tickets) and many of the technological requirements have been met.

We have argued elsewhere in this document that the safest system involves a closed system and a *patient*-held system operating at the same time. The one most persuasive argument for the closed system is that medical records can then evolve in their role as can attendant regulation, with progression toward the open or *patient*-held system if appropriate. None are 'ideal'.

The "Public interest" argument: potential abuse by the state.

Article 14(1) of the Commission of European Communities directive (CEC 1992) states that reasons for breaching confidence include public safety, the equivalent right of others, and monitoring procedures. This attitude is open to abuse by the state. This view is not new and it is commonly expressed[16]. For example, the document: "High Level Security Policy for Health Care Establishments" (1993) states the following circumstance in which the rights of *patients* may be overridden:

> "Where the public interest requires it, whether in a situation explicitly authorised by law, directly related to the protection of health, or necessary for state security or for the prosecution of criminal offences."

While this may be rational for data in general (CEC 1992) it is of concern where health care is concerned. People rarely consider the consequences of not respecting confidentiality. People's health data is already available to others by requesting medical reports from clinicians and bypassing this is difficult to justify. We oppose the part of this statement concerning state securityand assert that access to the record by the state should be under judicial control.

[16] British Journal of Health Care Computing 1993;10(6):10

The following may be deemed appropriate reasons for state intervention:

- subversive activity.
- criminal activity.
- for the purposes of public health.
- for political reasons.
- for evaluation of individuals.

All access to health care records must be made via the judiciary, and never directly by the state. Legislation should ensure this state of affairs.

Overly technological control of access

There is much speculation about the use of pin numbers by *patients* to control access to their record. Health care records are used a great deal when the *patient* is not present. Such procedures would require the *patient* to give the pin number to the *clinician*? What if the *patient* loses the pin number? What if the *patient* is unconscious or has reduced competence for other reasons? The 'smart card' will need sophisticated access control, but EHCRs at a HCF should be available to the *clinicians* providing care without the explicit consent of the *patient.* We have argued earlier that layers of access within the record controlled by such devices are unacceptable. The primary aim must be to improve clinical care.

Association of other functions with health care

The clinician may be a broker in many of the dealings the *patient* has with other organisations. Employers may request a report, the public housing authority may need verification of a medical condition before expediting housing or the police may want a statement about a *patient's* condition. All such activity should take place under strict professional codes and legislation, and require the written consent of the patient. Any compulsory association of other social functions with the provision of health care should be illegal.

Undifferentiated roles

There is a particular aspect of justice (McFarland 1991:73) which is not usually considered in health care, but is relevant in the context of the development of an EHCR. That is justice as the "fair distribution of benefits and burdens"; those who benefit the most from an innovation carry a fair burden of the risk. The *controller* is given the primary responsibility for the EHCR, and works with the *administrators* and *clinicians* to ensure the rights of individuals are protected. If the *controller* is also a *clinician* at an HCF it is possible that the interests of *patients* or *clinicians* may not be maximised, particularly if there is negligent use of the record. For these reasons we believe that the role of *controller* and *clinician* should not involve the same person.

Legislation designed to make people accountable for the records (with a consequent risk of litigation) must ensure that there are real benefits accrued by those individuals from using the EHCR. Failure to do so will result in a sudden halt in the development. *Administrators* and planners are also much less likely to have the co-operation of *clinicians* and *patients* if they perceive no benefit and co-ordinated processing of records may be severely restricted. The role of *controller* resolves this difficulty largely, as there is a clear duty to *patients* and *clinicians*.

Summary

There are potential problems with regulation, the most dangerous being intervention by the state outside the judiciary. Consideration of the sort of health care environment we want is also necessary. Regulatory bodies are essential to monitor abuse of the EHCR and to listen to concerns of users and *patients*.

Summary of laws relating to the EHCR:

Countries	Medical Secrecy/ Confident.	Access for Data Sets by Public Bodies	Sale of Data to third Parties	Exceptions to Medical Secrecy	Ownership of the Record	Control of the Record	Copyright of the Record	General Data Protection Act	Medical Exceptions to the Act	System Evaluation / Safety	Common Practice According to the Law
Belgium	Yes	Restricted	Unknown	Yes	?	Doctor	Doctor	Yes	Yes	?	Yes
Denmark	Yes	Yes, with Strict Rules	With Restrictions	Yes	Doctor / Patient	Doctor / Patient	Doctor	Yes	Yes	With Rules	Yes
France	Yes	Restricted	With Restrictions	Yes	Doctor	Doctor	Doctor	Yes	Yes	?	No
Germany	Yes	?	?	Yes	Doctor / Patient	Doctor / Patient	Doctor	Yes	Yes	?	No
Greece	Yes	Yes	Yes	?	?	Doctor	Doctor	No	No	?	Yes
Ireland	Yes	Yes with Rules	?	Yes	Doctor	Doctor	Doctor	Yes	Yes	?	No
Italy	Yes	Yes	Yes	Yes	Doctor	Doctor	Doctor	Yes	Yes	?	Yes
Luxembourg	Yes	Yes with Rules	?	Yes	Doctor / Patient	Doctor / Patient	Doctor	Yes	Yes	?	No
Netherlands	Yes	Yes with Rules	?	Yes	Doctor / Patient	Doctor / Patient	Doctor	Yes	Yes	Yes	Yes
Portugal	Yes	Yes with Rules	Yes	Yes	Doctor	Doctor	Doctor	Yes	Yes	No	No
Spain	Yes	Yes	?	Yes	Doctor	Doctor	Doctor	Yes	Yes	?	No
U.Kingdom	Yes	Yes with Rules	Yes with Rules	Yes	Doctor / Patient/ Health Serv.	Doctor / Patient	Doctor	Yes	Yes	Yes	No
Sweden	Yes	Yes with Rules	?	Yes	Doctor / Patient	Doctor / Patient / State	Doctor / State?	Yes	Yes	Yes	Yes
Finland	Yes	Yes with Rules	?	Yes	Doctor / Patient	Doctor / Patient / State	Doctor	Yes	Yes	?	?
Norway	Yes	Yes with Rules	?	Yes	Doctor / Patient	Doctor / Patient	Doctor	Yes	Yes	Yes	Yes
USA	Yes	Yes with Rules	Yes	Yes	Doctor / Patient / Institution	Doctor / Patient	Doctor	Yes	Yes	No	Complex Environment
Canada	Yes	Yes with Rules	?	Yes	Doctor / Patient	Doctor / Patient	Doctor	Yes	Yes	Yes	Yes

BIBLIOGRAPHY: EHCR - ETHICAL AND LEGAL IMPLICATIONS

AIM (1989), AIM Requirements Board. Impact Assessment and Forecasts of Information and Communications Technologies Applied to Health Care, Volumes I-IV ref XHI/F/A10966C, AIM Secretariat.

Allaërt FA, Dusserre L (1992), "Transborder flows of personal medical data in Europe: Legal and Ethical approach". in Medinfo 92, Lun K et al (Eds) Elsevier Science Publishers (North-Holland).

Anderson T, Jorgensen G. (1988) "Danish experience of statutory right of patients to access hospital records" [letter], Lancet 2:1428.

Anonymous. (1983) "Data protection: Council discusses interprofessional statement". BMJ 286: 1592.

Anonymous. (1993) "Why anonymous?" [editorial]. Lancet 341;1059-60

Audit Commission (1990) for Local Authorities and the National Health Service in England and Wales, "Survey of Computer Fraud and Abuse", United Kingdom.

Barber B. (1991) "Towards an information technology security policy for the NHS", in Current Perspectives in Health Care Computer 1991, Richards B et al.(Eds). British Computer Society, United Kingdom

Baskerville R. (1988) "Designing Information Systems Security", Wiley and Sons, Chichester, United Kingdom.

Bengtsson S, Solheim BG. (1992) "Enforcement of data protection, privacy and security in medical Informatics" in Proc. of the 7th World Congress on Medical Informatics (MEDINFO '92), K .C. Lun et al. (Eds), pp. 1561 -1565. Elsevier Science Publishers BV (North-Holland) Geneva 1992.

Berstein RA, Andrews EM, Weaver LA. (1981) "Physicians attitudes towards patients' requests to read their hospital records". Med Care 19;118-21

Biskup J., Bruggemann HH. (1988) "The Personal Model of Data: Towards a Privacy Oriented Information System", Computers and Security, Vol. 7(6): 575-97.

Branscomb A. (1991) "Common Law for the Electronic Frontier", Scientific American, pp112-5.

BMA, (1990) "Guidlines for doctors on the access to health records act 1990" British Medical Association, Tavistock Square, London WC1H 9JP, UK.

CEC. (1990), Commission of the European Communities, On the protection of individuals in relation to the processing of personal data, COM (90) 314 final, SYN 287, Brussels, September 1990.

CEC. (1991), Commission of the European Communities (Ed.), Directorate General XIII/F AIM, Data Protection and Confidentiality in Health Informatics, IOS Press, Amsterdam.

CEC. (1992), Commission of the European Communities, Amended proposal for a Council Direction on the protection of individuals with regard to the processing of personal data and on the free movement of such data, COM (92) 422 Final, SYN 287, Brussels, October 1992.

CEC. (1993), Procedings of the "AIM - CEN Workshop on the Medical Record" March 1993, Commission of European Communities DG XIII.

Council of Europe (1981), Convention on Protection of Individuals with regard to Automatic Processing of Personal Data, Strassbourg, France, January 28, 1991.

De Moor GJE, McDonald CJ, van Goor JN, (1993). "Progress in Standardisation in Health Care Informatics". IOS Press, Amsterdam.

DHSS (1985) Department of Health and Social Security. "Data protection act: subject access to personal health information". London UK.

Dick R, Steen E (Eds). (1991) Institute of Medicine. "The computer based medical record: an essential technology for health care". NAtional Academy Press, Washington.

Dusserre L, Allaërt FA. (1992) "Expert systems and medical liability" in Medinfo 92, Lun K et al (Eds) Elsevier Science Publishers (North-Holland) p 1576-81

Eloff J. (1988) "Computer Security Policy: Important Issues", Computers and Security 7(6):559-562

Fisher B, Britten N. (1993) "Patient access to records: expectations of hospital doctors and experiences of cancer patient". Br J Gen Pract 43:52-56

Gill M, Scott D. (1986) "Can patient benefit from reading copies of their doctors letters about them?" BMJ 293:1278

GEHR (1992), The Good European Health Record Project "Requirements for clinical comprehensiveness" Deliverable 4, AIM Project, DG XIII.

GEHR (1993), The Good European Health Record Project "The Clinical Functional Specification" Deliverable 7, AIM Project, DG XIII.

GEHR (1993a), The Good European Health Record Project "The Requirements for Medical Education" Deliverable 8, AIM Project, DG XIII.

Gritzalis D, Tomaras A, Katsikas S, Keklikoglou J. (1990) "Medical Data Protection: A Proposal for a Deontology Code", Joumal of Medical Systems, 14(6):375-386

Gritzalis D, Katsikas S. (1991) "Protection of Personal Information: Aims, Principles, Technical Issues", in Pro c. of the 2nd IFIP Conference on Govemmental and Municipal information Systems, North-Holland.

Gritzalis D, Katsikas S, Keklikoglou J, Tomaras A. (1992) "Determining Access Rights for Medical Information Systems", Computers and Security, Vol. 1(2):149 -161.

Gritzalis D, Katsikas S. (1992) "Data Confidentiality and Users Access Rights in Medical Information Systems", in Proc. of the 7th World Congress on Medical Informatics (MEDINFO ’92), K .C. Lun et al. (Eds), Elsevier Science Publishers BV (North-Holland) Geneva pp1566 -1571.

Hawkins C. (1985) "Mishap or Malpractice" Medical Defence Union, Blackwell Scientific Publications, Oxford.

Howell P.(1989), C4: Security and Privacy, CCTA Information Systems Guides, John Wiley and Sons, United Kingdom.

ITSEC. (1989) "Information Technology Security Evaluation; provisional harmonised criteria". The Commission of the European Communities, DG XIII, RACE programme.

Jackson J. (1991) "A practical guide to Medicine and the Law" Springer-Velarg, London.

Kapor M. (1991) "Civil-Liberties in Cyberspace", Scientific American, pp. 116 -120, September.

Kennedy I, Grubb A. (1989) "Medical Law: Texts and Materials", Butterworths, London.

Kowalski S. (1991) "The ABCs and Ds of National Computer Security Policies", Computers and Security, 10(3):213 -16.

Lobato de Faria, P. (1992) "Data protection and confidentiality in health informatics: a survey of legal issues in the EC community." Noothoven van Goor J, Christensen J, Eds. Advances in Medical Informatics, IOS Press.

McFarland MC. (1990) "Urgency of ethical standards intensifies in computer community" Computer March 1990;p77-81.

McFarland MC. (1991) "Ethics and the safety of computer systems" Computer February 1991;p72-75.

Pearce P, Parsloe P, Francis H, Macara A, Watson D. (1988) "Personal Data Protection in

Health and Social Services" Croom Helm, London.

Pfleeger SL. (1991) "A Framework of Security Requirements", Computers and Security, 10(6):515-523.

Post G, Kievit K. (1991) "Accessibility vs. Security: A Look at the Demand for Computer Security", Computers and Security, 10(4):331 -44.

RACGP. (1993) "Interim code of practice for computerised medical records in general practice". Royal Australian College of General practitioners, 39 Terry St., Rozelle, NSW, Australia 2039.

Randall T, Mant D. (1991) "Use of computerised general practice data for population surveillance: comparative study of influenza data" BMJ 302(6779):763-5

Robinson DM, (1992), "A legal Examination of Format, Signature and Confidentiality Aspects of Computerised Health Information" in Medinfo 92, Lun K et al (Eds) Elsevier Science Publishers (North-Holland).

Ross A. (1986) "The case against showing patients their records". [editorial] BMJ 292: 578.

Sherizen S. (1991) "European Unification ’92 Impacts on Information Security", Computers and Security, 10(7):601-10.

Simitis S.(1987) "Reviewing Privacy in an Information Society", University of Pennsylvania Law Review, Vol. 135, pp. 707 -746.

Turn R. (1990) "Information Privacy Issues for the 1990’s", in Proc. of the 1990 IEEE Symposium on Research in Computer Security and Privacy, pp. 394 -400, USA