

# **TAKING LIBERTIES IN CONFIDENCE**

**A REPORT FOR THE NUFFIELD TRUST ON THE  
IMPLICATIONS OF CLAUSE 67 OF THE HEALTH AND  
SOCIAL CARE BILL**

**Compiled and edited by  
Simon Davies  
Visiting Fellow  
Department of Information Systems  
The London School of Economics**

**March 2001**

## **TAKING LIBERTIES IN CONFIDENCE**

### **A REPORT FOR THE NUFFIELD TRUST ON THE IMPLICATIONS OF c. 67 OF THE HEALTH AND SOCIAL CARE BILL**

#### **SUMMARY**

1. Clause 67 of the Health and Social Care Bill contains powers under which regulations may be made to (a) control the processing of patient information, (b) prohibit or restrict the processing of prescribed patient information for commercial purposes, and (c) to require or regulate the processing of patient information for medical purposes in the interests of patient care or in the public interest.
2. The clause appears to have been drafted in response to (a) a perceived need to protect the economic interests of the NHS, (b) a desire to provide a legal foundation for greater control by government over the restriction or wider dissemination of healthcare data, (c) to provide protection of the functioning of cancer registries and other databases that operate without patient consent, and (d) to permit letters between clinicians to be copied lawfully to patients who are subjects of the correspondence.
3. Recent developments in health management in the UK, coupled with the use of powerful information technology, has created unprecedented threats to personal privacy. The principle of medical confidentiality has already been eroded to such an extent that in some areas of healthcare it is almost redundant. Clause 67 fundamentally weakens the few remaining safeguards for privacy.
4. The powers outlined in the clause are general in nature, and have been drafted in such a way that they can be exercised (within the constraints of law) in an almost limitless range of future applications, both for the disclosure of patient data, and for the withholding of patient data.
5. The clause has the effect of laying a legal foundation for an expansion of inter-agency data matching between, for example, the NHS, police, Social Services, Home Office and Benefits Agency. This process is expedited by the current work on protocols for information sharing of identifiable patient data between and beyond NHS organisations.
6. As currently drafted, clause 67 creates profound implications for the privacy of healthcare data. It has been long accepted that patient consent is the mechanism which best regulates the disclosure of personal health information. While the government maintains that it is committed to the idea of informed consent before disclosure, the effect and appearance of the clause will alter the foundation of this process.
7. Sub-Clause 67 (4) (c) which reads in part “..anything done by him in so processing the information shall be taken to be lawfully done despite any obligation of confidence owed

by him in respect of it” may cause permanent damage to the foundation of medical confidentiality by destabilising patient trust in the healthcare relationship.

8. Privacy and confidentiality underpin the trust between doctor and patient. If the quality of the doctor/patient relationship diminishes, it is inevitable that the quality and consistency of health data for medical research will be proportionately eroded. Further intrusions into patient privacy are likely to destabilise and diminish the value of medical research. There is overwhelming evidence that threats to confidentiality erode the level of trust between doctor and patient, and subsequently affect the quality and consistency of information provided by the patient
9. Traditionally, when the right of privacy is challenged by matters of public interest, stakeholders will engage through a constructive tension to achieve an outcome which rests on a strong ethical foundation. Clause 67 will substantially alter this formula by providing the Secretary of State with unprecedented powers that will, in effect, make the Minister the principal stakeholder. The effect will be to fundamentally alter the “patient centred” model of healthcare.
10. Widespread concern has been expressed that the provisions of clause 67 were drafted without the appropriate level of consultation with the general community or with healthcare and patient groups. Nor have draft regulations been presented for the consideration of Parliament – a matter of some concern in view of the general nature of the proposed powers.
11. One of the governments stated justifications for the provisions (i.e. that patient data can currently be processed without consent by commercial organisations) is irrelevant to the clause. The Data Protection Act provides wide ranging protections against such uses in the case of identifiable data, while truly anonymised patient data may lawfully and ethically be processed without compromising patient confidentiality.
12. Recent events such as the Harold Shipman case and the Alder Hey Inquiry highlight the importance of access to, and transparency of, certain healthcare data, particularly with regard to scrutiny of the NHS and activities within the NHS family. It is quite possible that these wide ranging powers in the hands of government may equally contribute to a corrosion of public confidence, leading to a reluctance to fully co-operate with clinicians.
13. Doctors are bound to respect the privacy of personal information entrusted to them by patients. Over recent decades, however, they have been required to disclose information for a wide and growing range of public interest purposes. The clause does not define the nature or extent of public interest, and thus it could be assumed that the definition might be indefinitely extended to cover administrative needs.
14. With the advent of new technologies, the functioning of both the cancer registries, and of nearly all medical research projects, is no longer dependent on the disclosure of identifiable health data. Techniques of anonymisation can maintain the integrity of data, as well as the integrity of medical privacy. Such technologies are in use throughout the world, and can be applied in the UK healthcare environment.
15. While the clause specifies that the powers will have regard for the provisions of the Data Protection Act (DPA), it is unlikely that the DPA will have any substantial limiting effect

on the new powers. Indeed the clause substantially weakens the current Data Protection Act exemption from informed consent, from a test of "necessity" to one of "reasonable practicality". This turns on its head the ethical basis of long-established conventions governing medical confidentiality.

16. The provisions of Clause 67, if implemented, are likely to lead to breaches of the Data Protection Act, the Council of Europe Recommendations on the Protection of Medical Data [R(97)5], and both Article 8 and Article 10 of the European Convention on Human Rights (the right to Privacy and the right to free flow of information and ideas)
17. On the basis of its representation and evidence, the Department of Health appears to have misunderstood the nature of data anonymisation, and indeed the position in law of anonymised data. This lack of understanding is a key failing in the quest to find practical solutions to the information challenges in the healthcare environment.

# 1

## INTRODUCTION

This report has been commissioned by the Nuffield Trust in response to concerns over the implications of clause 67 of the Health and Social Care Bill, currently before the House of Lords.

The clause contains powers under which regulations may be made to control the processing of patient information, to prohibit or restrict the processing of prescribed patient information for commercial purposes, and to require or regulate the processing of patient information for medical purposes in the interests of patient care or in the public interest.

Relatively early in the bill's passage through parliament, Donald Irvine, President of the General Medical Council and Ian Bogle, Chairman of Council of the British Medical Association (together with other colleagues) had written to the press warning that the clause "threatens patient confidentiality by giving the Secretary of State for Health wide and ill-defined powers to determine what information should be disclosed in the public interest or for the improvement of patient care, without patients' consent."<sup>1</sup>

This warning was followed by an open letter signed by a diversity of organisations including patients groups, computing organisations, and civil liberties alliances. The letter described the clause as "an attack on patient confidentiality".<sup>2</sup>

These concerns were echoed in part by the Delegated Powers and Deregulation Select Committee of the House of Lords, which expressed its concern over the wide ranging powers in the clause, and the lack of consultation in its drafting. The Committee was also concerned that the clause may breach the European Convention on Human Rights.<sup>3</sup>

This report is intended as an overview of the key issues that arise from the proposed powers in clause 67. A comprehensive legal analysis is beyond the scope of the report, though the key legal issues are presented. It is our intention to highlight areas of concern, and to provide a background to the issues of privacy and disclosure. The report also outlines some solutions that may satisfy the requirements of patient privacy and research interests.

I am indebted to Dr Ross Anderson, Dr Fleur Fisher, Dr Steve Hajioff, Dr Chris Pounder and Ian Brown for their contribution to this report, and to Dr William Lowrance, whose work on privacy and medical research has provided such an important input. Acknowledgements also go to the resources of the BMA and Privacy International.

---

<sup>1</sup> The Times, Letters, February 7, 2001

<sup>2</sup> Available at <http://www.gorjuss.com/medicalprivacy/archives/00000006.html>

<sup>3</sup> Report available at <http://www.publications.parliament.uk/pa/ld200001/ldselect/lddereg/45/4502.htm#a5>

## 2

**THE FRAMEWORK FOR PRIVACY AND CONFIDENTIALITY**

The provisions of clause 67 of the Health and Social Care Bill raise a number of key issues, including clinical autonomy, transparency and freedom of information. Yet there can be no doubt that the most complex and contentious implication of the clause is the potential for infringement of personal privacy.

Privacy has become one of the most important human rights issues of the modern age. At a time when computer based technology gives government and private sector organisations the ability to conduct mass surveillance of populations, privacy is seen as a crucial safeguard for individual rights.

According to opinion polls, concern over privacy violation is now greater than at any time in recent history.<sup>4</sup> Uniformly, populations throughout the world report their anxiety about encroachment on privacy, prompting an unprecedented number of nations to pass laws that specifically protect the privacy of their citizens. Intrusions on the privacy of healthcare data generally causes the greatest level of overall concern, and most developed countries have taken steps over the past decade to specifically protect the privacy and security of medical records.

The basis for this legal activity rests on a growing understanding that privacy is a fundamental right. Privacy is a value which underpins human dignity and other key values such as freedom of association and freedom of speech. These rights are established squarely in international covenants, and protected specifically in the constitutions of many nations.

The increasing sophistication of information technology, with its capacity to collect, analyse and disseminate information on individuals, has introduced a sense of urgency to the demand for legislation.

While the privacy of healthcare has traditionally been regarded highly by most people, it has been only in recent years that the public has expressed general concern over privacy violation in healthcare. Some of the reasons for this recent expression of concern are:

?? In recent years there has been a rapid increase in the amount, diversity, and intimacy of health-related data recorded.

?? Computerisation of health data storage, manipulation, linking, searching, transfer, and other processing continues to increase. This is bringing higher vulnerability to both accidental and intentional disclosure of sensitive data, and to misuse and abuse. The scale of health-related databases, and of prescribing and billing records, has increased

---

<sup>4</sup> Simon Davies "Re-engineering the right to privacy : how privacy has been transformed from a right to a commodity", in Agre and Rotenberg (ed) "Technology and Privacy : the new landscape", MIT Press, 1997 p.143

beyond all precedent, as has the interlinking and transferring of data among different, and different kinds of, databases, often at great distances;<sup>5</sup>

?? .Increasingly, health care is being provided by large, complex institutional and commercial systems. This is bringing much more auditing, analysis, and critical evaluation of healthcare practice and economics data, and increasing commerce in medical data per se.

?? The number and variety of parties seeking access to health data continue to increase, while the exemptions to confidentiality in the name of public interest has reached proportions which many people find alarming;

The protection of privacy has become the key means of allaying fears about these developments. In the healthcare environment, such protections are better known as “clinical confidentiality”.

### **The ethical basis of clinical confidentiality** <sup>6</sup>

The Hippocratic oath incorporated the principle of medical confidentiality into doctors' professional ethics. A modern statement can be found in the booklet 'Good Medical Practice' [GMC1] issued by the General Medical Council:

*Patients have a right to expect that you will not pass on any personal information which you learn in the course of your professional duties, unless they agree.*

This is expanded in the GMC booklet 'Confidentiality' which stipulates that doctors who record or who are the custodians of confidential information must ensure that it is effectively protected against improper disclosure.

Both the government and the healthcare unions are agreed that electronic health records must be at least as well protected as paper ones; the Data Protection Act makes GPs and others responsible for the security of personal health information that they collect; and a recent EU Directive obliges the government to prohibit the processing of health data except where the data subject has given his explicit consent, and in certain other circumstances

The basic ethical principle, as stated by both the GMC and the EU, is that the patient must consent to data sharing. The ethos surrounding research on humans was recast and codified after World War II, as the world coped with the revelation of the medical atrocities perpetrated by the Nazis.<sup>7</sup> The resulting “Nuremberg Code”—the opening sentence of which was, “The voluntary consent of the human subject is absolutely essential”—established principles having to do with the purposes of the research,

---

<sup>5</sup> Lowrance, W; Privacy and Health Research

<sup>6</sup> Edited extract from Ross Anderson's “Security in Clinical Information Systems” at <http://www.cl.cam.ac.uk/users/rja14/policy11/policy11.html>

<sup>7</sup> Lowrance, W

gauging of risk and benefit to the subject, qualifications of researchers, and subject rights generally.<sup>8</sup> Consent is central in all privacy negotiations.<sup>9</sup>

Confidentiality is the privilege of the patient, so only he may waive it. Furthermore, the consent must be informed, voluntary and competent. Thus, for example, patients must be made aware that information may be shared between members of a care team, such as a general practice or a hospital department.

A number of exceptions to this rule have developed over time, and include both statutory requirements and exemptions claimed on pragmatic grounds; they pertain to the notification of abortions, births, some deaths, certain diseases, adverse drug reactions, non-accidental injuries, fitness to drive and disclosure to lawyers in the course of a dispute (see next chapter). There is controversy over research; the NHSE claims that by seeking treatment, a patient gives implied consent to the use of his records in research, while the healthcare professions do not accept this.

### **The legal context**

Privacy is generally viewed as fundamental (though not an absolute) human right. The concept can be traced as far back as 1361, when the Justices of the Peace Act in England provided for the arrest of peeping toms and eavesdroppers.<sup>10</sup> Various countries developed specific protections for privacy in the centuries that followed. In 1792, for example, the Declaration of the Rights of Man and the Citizen declared that private property is inviolable and sacred.

The modern privacy benchmark at an international level can be found in the 1948 Universal Declaration of Human Rights, which specifically protected territorial and communications privacy. Article 12 states : "No-one should be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks on his honour or reputation. Everyone has the right to the protection of the law against such interferences or attacks".

Numerous international human rights covenants give specific reference to privacy as a right. The International Covenant on Civil and Political Rights reinforced the UDHR, while the European Convention on Human Rights expands the concept to "private life".

In Britain, confidentiality has been evolving in law since 1910, when doctors began arguing with successive governments over access to medical records. The compromise that has emerged over the years balances patient privacy, professional autonomy, public health effectiveness, and scientific research. Past attempts to disturb this balance have foundered - on professional resistance, on patient rights and on the property rights of healthcare firms. But the side-effects of these disputes have often been severely debilitating.<sup>11</sup>

---

<sup>8</sup> *Trials of War Criminals before the Nuremberg Military Tribunals under Control Council Law No. 10*, volume 2, pp. 181–182 (U.S. Government Printing Office, Washington, DC, 1949).

<sup>9</sup> Lowrance, W

<sup>10</sup> James Michael, p.15

<sup>11</sup> British Medical Journal, February 24th: Undermining data privacy in health information

Most notable among these disputes was the last government attempt to extend its access to personal health information. This was the the IM&T (Information Management & Technology) strategy, which in 1992 talked of a single electronic health record, accessible to all within the NHS. But the strategy was not designed to facilitate health data sharing between physicians, so much as its collection in central databases. This put the strategy on a collision course with the law. For example, the Venereal Diseases Act restricts identifiable data on sexually transmitted diseases to the patient and the provider; yet the NWCS Contract Minimum Dataset contains the HIV status of the patient - even where this is irrelevant to treatment <sup>12</sup> This episode so undermined confidence in the confidentiality of NHS networking that it delayed the introduction of IT into the NHS by several years.<sup>13</sup>

In Britain, as in all European countries, the protection of privacy is enshrined primarily in Data Protection law (in the case of the UK, the Data Protection Act, 1998). It sets out a number of principles aimed at safeguarding personal data, and specifies that information should be:

- ??obtained fairly and lawfully
- ??used only for the original specified purpose
- ??adequate relevant and not excessive to purpose
- ??accessible to the person it relates to
- ??accurate and up to date, and
- ??destroyed after its purpose is completed

The Data Protection Act places strong emphasis on the notion of consent, a provision which has been long upheld in the health environment.

It is against this background that the implications of clause 67 can be viewed. The clause is likely to accelerate the erosion of privacy by undermining the core principle of patient consent. It cannot be assumed that the Data Protection Act will provide any significant level of protection. The Act can be rendered ineffective in the face of overriding legislation, leaving patients with little or no rights over their personal information. The Human Rights Act, on the other hand, may be invoked as a mechanism to challenge actions by government which are considered arbitrary or unfair. Legal opinion on the compatibility of the Regulation of Investigatory Powers Act with the ECHR indicates that a case may successfully be brought against the government over clause 67.<sup>14</sup>

---

<sup>12</sup> Contract minimum dataset includes confidential data. OM Goodyear, BMJ 1996; 312: 185 <<http://www.bmj.com/cgi/content/full/312/7024/185>>

<sup>13</sup> Ross Anderson; "Security in Clinical Information Systems" at <http://www.cl.cam.ac.uk/users/rja14/policy11/policy11.html>

<sup>14</sup> at <http://www.fipr.org/rip/index.html>

## 3

**PRIVACY AND THE PUBLIC INTEREST**

Privacy may elude definition, but it is without doubt a deeply held idea throughout society. The concepts of “personal matters” and “intimate knowledge” are familiar, as is the notion that individuals live in a “private sphere” over which they should have autonomy.. Everyone believes that some, indeed many, core aspects of life “are nobody else’s business.” Yet what one person is fiercely secretive about, another may openly reveal.<sup>15</sup>

This difference in outlook forms the bedrock of arguments for public interest exceptions to the right of privacy and confidentiality. This tension is often expressed as an equation that attempts to balance the privacy rights of an individual, weighed against other interests of other individuals or society. In its crudest expression, the demands for privacy by one individual may compromise the rights of other individuals, and must be sacrificed. The sacrifice is generally codified in law, and is known as an exemption.

Sub-clause (3) (b) of clause 67 specifies that the Secretary of State may exercise his power in cases of overriding public interest. Public Interest is not defined in the Bill, but its scope is extremely broad, and likely to become broader in the future (see below).

A doctor’s duty to protect confidentiality has never been absolute, but prior to the 20<sup>th</sup> century, the conditions for breaching confidence without patient consent fell generally into three relatively uncomplicated categories:

??**Disclosure** of details to the patient’s family (specifically where the patient needed support or care);

??**Discussion** of the patient’s condition with another doctor (particularly to seek further information or to report findings);

??**Alerting** people who may be adversely affected by the patient’s condition (particularly with regard to infectious diseases).

With the increasing integration of healthcare, and its constantly expanding presence, the parameters for disclosure of personal information have increased. The passage of legislation has likewise reflected the presence of a larger range of public interest issues in which medical data is seen as playing a key role. Doctors are now required – often by law – to disclose confidential information (without the patients consent) in a wide range of circumstances. These include:

**Disclosure to prevent Serious Harm**

This information may be required for the protection of identifiable individuals or to society at large. The BMA has identified threats to living people as significant in a way in which threats to property or financial interests are not. In line with this reasoning, the

---

<sup>15</sup> Lowrance, W; Privacy and Health Research; Report to the U.S. Secretary of Health and Human Services, May 1997 <http://aspe.hhs.gov/datacncl/PHR.htm>

risk of an assault, a traffic accident or an infectious disease might be seen as more compelling grounds for disclosure than the risk relating to fraud or theft. . These include murder, manslaughter and rape. Serious harm, however, is a much wider concept than that of serious criminal activity and it encompasses omissions, such as neglect, as well as acts. It must also take account of psychological as well as physical damage. Child neglect or abuse is an example of treatment whose psychological sequelae may be considerably more profound than the physical harm suffered and the psychological damage may be experienced not only by the actual victim but also by siblings who know of it.<sup>16</sup>

**Disclosure required by a court.** Doctors may be held in contempt of court if they refuse to disclose health data demanded by a court of law. The key categories here are:

- ?? disclosure for litigation purposes
- ?? disclosure in criminal cases
- ?? disclosure to a coroner's court
- ?? military law and regulations
- ?? disclosure by police surgeons

### **Laws affecting all citizens**

In addition to laws specifically requiring disclosure from health professionals, they may also be affected by the disclosure statutes which affect all citizens. Examples are the obligation under the Prevention of Terrorism (Temporary Provisions) Act 1989 to inform the police of information about terrorist activity, and the Road Traffic Act 1988's requirement to provide the police, on request, with information which might identify a driver alleged to have committed a traffic offence.

### **Serious crime and national security**

Disclosure necessary for the prevention, detection, investigation or punishment of a serious offence is widely regarded as justifiable and desirable. The definition of what constitutes a "serious" crime is a matter of debate. The Police and Criminal Evidence Act 1985 contains some definitions of what it calls a "serious arrestable offence", that is one which has caused or may cause serious harm to the security of the state or to public order; serious interference with the administration of justice or with the investigation of an offence; death; serious injury; or substantial financial gain or serious loss. (Police and Criminal Evidence Act 1985 (s 116)). These definitions include such crimes as murder, manslaughter, rape, treason and kidnapping.<sup>17</sup>

### **Adverse drug reactions**

Mechanisms exist for the routine reporting of adverse drug reactions to the Medicines Control Agency. The reporting system requires the inclusion of the patient's name, sex and date of birth as well as details of the reporting health professional.

### **Disclosure in the interests of Public health**

Public health doctors may need to disclose information about an individual in order to identify the source of an infection or other possible carriers. Statutory requirements for notification in such cases may not cover all of the measures necessary to protect public

---

<sup>16</sup> ibid

<sup>17</sup> ibid

health but the public health doctor may decide that disclosure is justified to prevent a serious threat to other people or to protect public safety. In some cases no particular individual is perceived to be at risk from non-disclosure but there may be a generalised threat. This can be sufficient justification for disclosure if there are real grounds to suppose that harm may come if the information is not revealed.

### **Disclosure in the interests of Public safety**

A common example of what can be categorised as public safety occurs in connection with the assessment of patients with, for example, diabetes, epilepsy, defective eyesight or serious cardiac conditions who have been advised by health professionals to discontinue driving but who nevertheless continue.<sup>18</sup> Health professionals must consider whether non-disclosure in relation to a foreseeable and serious threat might leave them open to a possible charge of negligence if grave harm results from the non-disclosure. Issues of public safety may similarly arise in circumstances where an individual legitimately possessing firearms is thought by health professionals to be a risk because of drug or alcohol addiction or a medical condition such as depression.<sup>19</sup>

### **Safety in the workplace**

Disclosure is justifiable where failure to do so in regard to the health status of an employee could foreseeably result in a substantial risk to others. For example an occupational health doctor has a responsibility to take action if he or she is aware that the health of an employee threatens the safety of others. Similarly, GPs may need to take action if they become aware that a patient they consider to be a threat to vulnerable people begins working with young children, the elderly or other vulnerable groups.

### **Abuse and neglect**

The need to disclose information to protect children or vulnerable adults may arise if there is suspected abuse, neglect or non-accidental injury. In any case where abuse is suspected, the vulnerable person's wellbeing is paramount, and the promotion of such should be the motivating factor in any decision to disclose.

## **NON STATUTORY PRESSURES ON DISCLOSURE**

Beyond statutory demands for disclosure of information are numerous circumstances where doctors are expected to disclose in the public interest (or where failure to do so leaves them open to prosecution). These include:

**Quasi-law** means standards to which health professionals are expected to adhere, contained in, for example, guidance from non-statutory professional bodies, health service circulars and executive letters, even where these are not legally binding<sup>20</sup>. These may have varying degrees of legal force by virtue of the manner in which they set standards, or of their relationship to statute. In practice, they are very influential and usually can be seen as representative of a responsible body of opinion within the health professions. Department of Health guidelines on the requirements for research ethics

---

<sup>18</sup> . Confidentiality, GMC, October 1997: para 19 and appendix I

<sup>19</sup> Interim firearms guidance note, BMA, 1996

<sup>20</sup> Quasi-law is discussed in Health care law, Montgomery J, OUP, 1997, Chapter 1. See also Quasi-legislation: Recent developments in secondary legislation, Ganz G, Sweet and Maxwell, 1987)

committee approval of research, and on the retention of health records are examples of quasi-legal rules in relation to confidentiality.<sup>21</sup>

**Research requirements** Doctors are frequently asked to provide patient data for research purposes. While the guidelines for such disclosure are set out clearly by such organisations as the GMC and the BMA, there is substantial doubt on such issues as anonymisation and consent

### **Disease registers**

Disease management registers are databases holding information about patients usually for purposes of that patient's care. Registers may also be used to provide non-identifiable information for planning the use of health service funds and for research. An example would be a register holding information about diabetic patients, which included information about care plans and correlated this with information about use of health care services. It can thus be used to monitor that individual's health, and the information can be used to make comparisons between different care plans and whether these lead to differences in the need to access health care services.

### **Medical reports for fertility treatment**

Most available guidance confines its concerns to the threat to existing people. However, requests for medical reports in connection with the provision of fertility treatment sometimes raise questions of doctors' duties to have regard for the wellbeing of children who might be born as a result of reproductive services.<sup>22</sup>

**Other areas** in which patient data may be requested or accessed include clinical audit, teaching, genetic registers, complaints procedures, planning, administration & purchasing and financial audit

Given this wide spectrum of conditions for disclosure, there is a strong argument for defining and circumscribing the concept of public interest, rather than providing new mechanisms to expand it. The powers in clause 67 clearly provide the potential for the government to extend the scope of public interest exemptions, with the bare minimum of safeguards and consultation.

---

<sup>21</sup> Local research ethics committees, HSG (91) 5; Ethics committee review of multi-centre research, HSG (97) 23; Preservation, retention, and destruction of GP general medical services records relating to patients, HSC 1998/217).

<sup>22</sup> BMA confidentiality advice

## 4

**TRUST, ANONYMITY AND THE RESOLUTION OF PUBLIC INTEREST**

The popular view of “public interest” is, however, not entirely adequate in the context of medical confidentiality. There is also, as the BMA has pointed out, a public interest argument for strong and resilient confidentiality. In addition to the traditional duty of medical secrecy which has been incorporated into the professional codes of health workers, there is also a strong public interest in maintaining confidentiality so that individuals will be encouraged to seek appropriate treatment and share information relevant to it. Part of the BMA’s emphasis on confidentiality and young people, for example, is based on the fact that minors are likely to avoid consulting health professionals for contraception, abortion, treatment of sexually transmitted infections or substance abuse where they are not confident of the privacy of the consultation. Similarly the BMA has opposed proposals that doctors should become involved in reporting suspected illegal immigrants who present for treatment, partly because it believes doctors should not be seen as agents of the state in such matters and also because of the potential public health consequences of discouraging such patients from seeking medical advice.<sup>23</sup>

A strong culture of confidentiality is also valuable for society at large. Sub-Clause 67 (4) (c) grants immunity for doctors who breach confidentiality, and places government demands for information above the duty of care. It reads in part “..anything done by him (the doctor) in so processing the information shall be taken to be lawfully done despite any obligation of confidence owed by him in respect of it”. While this may be an expedient means of avoiding the legal duty of confidence, the provision may cause permanent damage to the foundation of medical confidentiality by destabilising patient trust in the healthcare relationship.

Privacy and confidentiality underpin the trust between doctor and patient. The assurance that revelations made within the healthcare relationship will be held confidential encourages people to seek care in the first place, and then to be open in the exchanges involved—divulging information truthfully, asking questions even though doing so may be awkward or embarrassing, co-operating with procedures, and generally nurturing mutual confidence in the relationship. This is essential to effective health care, including public-health surveys and many other activities beyond primary care. In his study for the US Department of Health, William Lowrance noted “During the course of this study the author was dismayed at the number of people, encountered in passing, who mentioned that they have stopped going to their gynaecologists, for instance, or mistrust screening or counselling programs, or are reluctant to ask reimbursement for health care, because they “know” that medical confidences will not be respected, or because they fear negative discrimination”. Similar scenarios have arisen in aspects of STD and other disease notification procedures.

---

<sup>23</sup> Advice on confidentiality and disclosure. Published on the website of the British Medical Association (BMA) at [www.bma.org.uk](http://www.bma.org.uk)

If the quality of the doctor/patient relationship diminishes, it is inevitable that the quality and consistency of health data for medical research will be proportionately eroded. Further intrusions into patient privacy are likely to destabilise and diminish the value of medical research. There is overwhelming evidence that threats to confidentiality erode the level of trust between doctor and patient, and subsequently affect the quality and consistency of information provided by the patient

There are many conditions in which informed and explicit consent by patients can result in the strengthening of trust between clinician and patient, and consequently, high quality data being used productively in research. Consent is a cornerstone both of data protection law, and of the guidance issued by bodies such as the GMC.

However, there are circumstances where explicit consent is deemed undesirable or is not possible (though it must be said that these circumstances are much more rare than is claimed by some research bodies and disease registries). In these cases, doctors are urged to anonymise patient data, so that the identity of subjects can never be revealed.

The standard way of protecting such information is to remove patients' names and addresses from their records and thus make them anonymous. But this is rarely sufficient. If a database allows sufficiently detailed queries, then individuals can still be identified, and this is especially so if information about different clinical episodes can be linked. For example, if I am trying to find out whether a politician born on the 2<sup>nd</sup> June 1946 and treated for a broken collar bone after a college football game on the 8<sup>th</sup> May 1967, had since been treated for drug or alcohol problems, and I could make an enquiry on those two dates, then I could very probably pull out a single medical record from a national database. Even if the date of birth is replaced by a year of birth, I am still likely to be able to compromise patient privacy if the records are detailed or if records of different individuals can be linked. For example, a query such as 'show me the records of all women aged 36 with daughters aged 14 and 16 such that the mother and exactly one daughter have psoriasis' is also likely to narrow down the search to one individual out of millions. However, complex queries with lots of conditions are precisely the kind that researchers want to make.<sup>24</sup>

For this reason, the US Healthcare Finance Administration (HCFA), which is responsible for paying doctors and hospitals for treatments provided under the Medicare program, maintains three sets of records. There are complete records, used for billing. There are {\em beneficiary-encrypted} records, with only patients' names and social security numbers obscured. These are still considered personal data (as they still have dates of birth, postal codes and so on) and so are only usable by trusted researchers. Finally there are {\em public-access} records which have been stripped of identifiers down to the level where patients are only identified in general terms such as 'a white female aged 70-74 living in Vermont'. Nonetheless, researchers have found that many patients can still be identified by cross-correlating the public access records with commercial databases, and following complaints by privacy advocates, a recent report from the General Accounting Office criticised HCFA for lax security.<sup>25</sup>

---

<sup>24</sup> From Security Engineering -- A Guide to Building Dependable Distributed Systems  
Ross J Anderson Wiley, February 2001

ISBN 0-471-38922-6

<sup>25</sup> General Accounting Office, USA, 'Medicare —Improvements Needed to Enhance Protection of Confidential Health Information', GAO/HEHS-99-140;

Many other countries have healthcare monitoring systems which use similar technologies. New Zealand has a national database of encrypted-beneficiary medical records, with access restricted to a small number of specially cleared medical statisticians. No query is answered with respect to less than six records.<sup>26</sup> Germany has very strict privacy laws, and the fall of the Berlin Wall forced the former East German cancer registries to install protection mechanisms rapidly.<sup>27</sup> In other countries, protection has been less adequate. Britain's National Health Service started out with strict guidelines but then built a number of centralised databases which make personal health information widely available within government and which have led to confrontation with doctors.<sup>28</sup> Similar systems in Switzerland were replaced at the insistence of local privacy regulators.<sup>29</sup> The most controversial of all has been a genetic database in Iceland, which we'll discuss below.

De-identifying personal information is important in many other fields. Under the rubric of 'Privacy Enhancing Technology' it is being promoted actively by regulators in Europe and Canada as a general privacy mechanism. But there still remains a tension between the desire of researchers for detailed data, and the need to limit the detail in order to protect privacy. That is why such mechanisms are not sufficient on their own.

A prominent case at the moment is a new medical research database in Iceland. There will in fact be three linked databases: one with the nation's medical records, one with the genealogy of the whole population, and one with genetic data acquired from sequencing. The rationale is that since Iceland's population is largely descended from a few founding families who settled there about a thousand years ago, there is much less genic variance than in the general human population and so genes for hereditary illnesses should be much easier to find.

The privacy problem in the Icelandic database is much more acute than in the general case. For example, by linking medical records to genealogies, which are in any case public (genealogy is a common Icelandic hobby), patients can be identified by such factors as the number of their uncles, aunts, great-uncles, great-aunts and so on—in effect by the shape of their family trees. There was much debate about whether the design could even theoretically meet legal privacy requirements<sup>30</sup> and European privacy officials expressed grave concern about the possible consequences for Europe's system

<http://www.gao.gov/AIndexFY99/abstracts/he99140.htm>

<sup>26</sup> "Managing Health Data Privacy and Security", R Neame, in 'Personal Medical Information—Security, Engineering and Ethics', Springer-Verlag (1997) ISBN 3-540-63244-1 pp 225--232 {Blo97}

<sup>27</sup> "Clinical record Systems in Oncology. Experiences and Developments on Cancer Registers in Eastern Germany", B Blobel, in Anderson (op. cit.) pp 39--56;

<http://www.cl.cam.ac.uk/ftp/users/rja14/blobel.pdf>

<sup>28</sup> RJ Anderson, "Safety and Privacy in Clinical Information Systems", in {em 'Rethinking IT and Health' }, J Lenaghan {em (ed.)}, IPPR (Nov 98) (ISBN 1-86030-077-4) pp 140—160

<sup>29</sup> M Schnyder, "Datenflüsse im Gesundheitswesen", in in Symposium fuer Datenschutz und Informationssicherheit, Zuerich, Oct 98

<sup>30</sup> RJ Anderson, "The DeCODE Proposal for an Icelandic Health Database", The Icelandic Medical Journal v 84 no 11 (Nov 98) pp 874-5;

<http://www.cl.cam.ac.uk/users/rja14/#Med>

of privacy laws.<sup>31</sup> However, the Icelandic government pressed ahead with it anyway over the strong objections of local doctors.

The effect of this has been that 11% of the Icelandic population has opted out of the database (and this includes over half of all doctors). A further effect has been a loss of confidence in the project, which in turn has led to a severe fall in the share price of the operating company.

### **Another solution: Pseudonymisation**

That every patient has a right to confidentiality is not contentious. In some cases, however, society has historically compromised that right in favour of service efficiency or the greater good. Whilst the altruistic arguments still apply, it is increasingly untenable to disclose information in the absence of informed consent. Whilst the patient record was a physical thing, requiring strength to carry and time to search, doctors could rely on physical means to afford some protection of patient data. Changes in technology have facilitated the disclosure of patient data and have increased the importance of measures to protect patient privacy. As has been seen in the recent cases with regard to the retention of organs, it is not sufficient to cite implied consent. Furthermore, if implied consent is deemed as sufficient, this is likely to effect some of the information disclosed to clinicians and have an adverse effect on clinical care. Consent needs to be full and informed. Furthermore, blanket consent is unlikely to be acceptable – another inference that can be drawn from the recent issues about post mortem examinations - separate consent will be needed for each disclosure.

With the introduction of fully informed consent into standard data sharing practice, it is likely that some patients will deny consent and that this may vary by patient group, hence injecting a systematic bias into the data. Further to this is the change in assumption. Under current practices, consent to share information is assumed; clearly we are moving towards the opposite, where refusal will be assumed unless explicit consent is granted. Through this process, non-responders become non-consenters. This will lead to further bias and degradation of data quality. In addition to this, it is likely that sequential data requests will be received less favourably, and the likelihood of response will thus decrease with number of requests and thus with increasing morbidity. Finally, the process of collection and recording of consent is likely to be extremely labour intensive.

Researchers thus have three reasons for difficulty with the use of identifiable patient data; the ethical tensions, the administrative difficulties and the negative impact on data quality. For these reasons, there needs to be a careful assessment and a minimisation of the instances where identifiable data is used.

### **Types of data**

One of the problems that researchers face is a historical lack of understanding of the difference between identifiable data and individual data. The research community has often used identifiable data where individual data would have sufficed. Identifiable data is information that can be tracked down to an individual or small group of individuals.

---

<sup>31</sup> Two statements, made by the Data Protection Commissioners of EU and EES countries and Switzerland, 20<sup>th</sup> International Conference on Data Protection, Santiago de Compostela, 16-18 September 1998; available at <http://www.dataprotection.gov.uk/20dpcom.html>

Individual data is data that pertains to one patient; it need not contain any information as to the identity of that patient

Whilst there are unlikely to be ethical problems with the use of aggregated anonymised data (as long as the anonymisation is robust) the epidemiological and organisational usefulness of the data is limited to ecological comparisons and thus subject to cluster effects, ecological fallacy and casemix. For this reason, it is unlikely that this form of data will be sufficient for quality assurance or for anything but the most basic epidemiological research.

Notwithstanding the issues outlined above, it is clear that for much direct patient care, only fully identifiable patient data will suffice. In between these lie a number of areas for which there is a need for individual patient data but there is not usually a need to be able to identify the patient. It is within these areas that pseudonymisation is useful. Areas of work such as audit and quality assurance, epidemiological and syndromic surveillance and epidemiological research can rely upon pseudonymised data for their day to day function.

On this basis, a chronic disease management system that is being used to co-ordinate the shared care of individual patients needs to use identified data (although there needs to be a means whereby access is strictly controlled and identifiable data can not be aggregated). On the other hand, a chronic disease register whose function is quality assurance or audit of care practices and outcomes can function more effectively (and ethically) with pseudonymised data. Clearly if, during a quality assurance process, a failure in the system is found that has implications for individual patients, there will be a need to remove the pseudonymisation from those individuals so that they may be identified by appropriate parties and appropriate action taken.

In order for there not to be a need for individual consent, pseudonymisation must be secure and complete. Simply to use the NHS number as a pseudonym is insufficient; as it is a number that is relatively accessible and thus insufficiently pseudonymous. Likewise, the use of a single pseudonym for all references to an individual patient is insufficiently secure, and can lead to the inappropriate distribution of sensitive information (for example genito-urinary medicine information. A secure pseudonym would require the allocation of a novel alphanumeric code for each request for each data item. On this basis, any data linkage would have to take place through the pseudonomising body. It would thus be impossible to reconstruct or link any data without appropriate authorisation. The database at the pseudonomising body would contain the identifiers and the pseudonyms allocated to that individual for each data request. It would contain no clinical data.

On this basis, detailed patient data, stripped of all identifiers, could be disclosed and used for quality assurance or epidemiological purposes prior to obtaining patient consent. Consent need only be obtained if pseudonymisation needs to be broken. It should also be noted that there may be some instances where pseudonymisation needs to be broken in the absence of individual consent, in an outbreak of serious infection or at the request of a court, for example. There is a need for specific practices to deal with these eventualities.

An added advantage of such processes over the current practices of semi-secure networks is the additional ability to perform data linkage with information from outside normal

NHS channels without compromising patient confidentiality. This could provide a research tool and a disease surveillance instrument of significant power.

A system of secure pseudonymisation would be one efficient and effective means of ensuring good quality information for the purposes of quality assurance whilst safeguarding the right of patients to privacy and the duty of clinicians for confidentiality. The provision of such systems should be explored as a matter of priority.

### **The pathology of disclosure**

The research community has failed to take advantage of such developments in secure and anonymous record management. This situation can be traced in part to an innate hostility to the concept of privacy, and an almost pathological belief in the primacy of identifiable data. Rather than moving toward the ideal of strengthening patient trust through informed consent, disease registers and researchers often attack the notion of informed consent, claiming that identifiable data is crucial to their work, and that consent would paralyse research.<sup>32</sup>

In a recent briefing document, the UK Association of Cancer Registries (UKACR) claimed that informed consent is unworkable and, if it was required, would “result in an unquantifiable loss of information”.

The UKACR says that future research projects using retrospective records would be disabled as a result of the Data Protection Act’s requirement for consent to be tied to a specified purpose. Asking for consent “that is adequately broad for [not yet known] research is unlikely to be legally acceptable”, it says.

Another legal barrier, the organisation claims, is that consent is unlikely to have lifetime validity. Individuals’ records on cancer registers remain active until the death of the data subject - so renewal of consent would, therefore, be needed at every NHS contact, says the briefing document.

The UKACR argues that their records need to be person identifiable for the following reasons:

- ?? linking dispersed records of a patient’s lifetime journey through healthcare encounters. (The NHS number is not yet universally applied; is not always accurate; and cannot yet provide adequate anonymisation.);
- ?? tracing familial relationships. This, though, does require the explicit, informed, consent of data subjects; and
- ?? “registries also supply names of patients to bona fide researchers for detailed research projects” relating to specific cancers. Although ethics committees and patients’ care teams are involved in approval processes, data subjects are not. Patients are approached, usually via their GPs, for further information only, when they are informed and invited to give their consent to the inclusion of additional information.

It is for these very reasons that registries should support the idea of both consent and anonymisation. To seek a blanket exemption in law would result in a corrosion of trust between patients and the health service. Ultimately (for reasons explained above) the quality and value of research would be diminished.

---

<sup>32</sup> Available at <http://www.gorjuss.com/medicalprivacy/archives/00000023.html>