Organisational & Confidentiality Issues

By Robin Beaumont

robin@organplayers.co.uk

17/06/2003 15:24

N. Narou-Romain. Plan for a penitentiary, 1840 A prisoner, in his cell, kneeling at prayer before the central inspection tower (in Micheal Foucault 1979 discipline & Punish pp162 penguin books)

http://www.leksikon.org/art.php?n=945
Contents

1. INTRODUCTION ............................................................................................................................................. 3

2. THE PANOPTICON ........................................................................................................................................... 3

   2.1 WEB LINKS ............................................................................................................................................... 6

3. TECHNOLOGICAL DETERMINISM .................................................................................................................. 7

4. MANAGERIAL STRATEGIES ............................................................................................................................. 8

5. FREEDOM OF INFORMATION AND THE DATA PROTECTION ACT (DPA) ................................................. 9

   5.1 CALDICOTT .............................................................................................................................................. 12

6. CLINICAL GOVERNANCE ............................................................................................................................... 14

   6.1 THE STRUCTURE ..................................................................................................................................... 14

   6.2 THE PROCESS ......................................................................................................................................... 15

7. TASK UNCERTAINTY AND COMPLEXITY ..................................................................................................... 16

   7.1 SUMMARY .............................................................................................................................................. 17

8. REFERENCES ....................................................................................................................................................... 18

Document details ....................................................................................................................................................... 19
1. Introduction

As professionals gaining a working knowledge of the social aspects of Informatics is essential. While learning the basic skills of how to use computers provides an insight into how they might support and influence work tasks it does little in addressing directly the social issues concerning Informatics. This aspect of Informatics is a highly complex subject area, spanning numerous disciplines such as sociology, psychology, medical ethics, Artificial intelligence (AI) and a host of newer disciplines such as situation theory introduced in the chapter on information and knowledge. Presented below are only a few pertinent topics. The approach taken is one of introducing the most general issues first and then gradually moving into areas which are specific to medicine.

2. The Panopticon

Kilmainham Gaol, Dublin: a 'panoptic' prison? From http://www.ucl.ac.uk/Bentham-Project/Faqs/fpankilmainham2.htm

Sir Jeremy Bentham's Panopticon (1748-1832),

Panopticon fængsel. Interiør fra Stateville fængslet i USA

From http://www.leksikon.org/art.php?n=945
The Panopticon was a central vantage point in prisons designed in a circular fashion during the 19th century. For an illuminating description along with illustrations of these central towers see Foucaults Discipline and punishment (p.251). Zuboff analyses the technology revolution in terms of the characteristics of a panoptican.

Zuboffs basic premise is:

"a powerful new technology, such as that represented by the computer, fundamentally reorganizes the infrastructure of our material world. It eliminates former alternatives. It creates new possibilities. It necessitates fresh choices. The choices that we face concern the conception and distribution of knowledge in the workplace. . . . The choices that we make will shape relations of authority in the workplace . . . .The new technological infrastructure becomes a battle field of techniques, with management inventing novel ways to enhance certainty and control, while employees discover new techniques of self protection and even sabotage . . . . Computer based technologies are not neutral: they embody essential characteristics that are bound to alter the nature of work with our factories and offices, and among workers, professionals, and managers. New choices are laid open by these technologies and these choices are being confronted in the daily lives of men and women across the landscape of modern organisations."

**Exercise:**

Give some examples of the 'battle field'.

What do you think Zuboff means by saying 'Computer based technologies are not neutral'. Have you come across any examples of this?

The above premise that Zuboff puts forward contains a wealth of knowledge and could easily become a complete course in its-self. The acceptance that Information Systems are not value free has fundamental effects upon the methods used to design, implement and evaluate them and some of these implications will be discussed in the other sections concerned with the social issues of Informatics particularly those sections on participative design methods and information centres in other documents. But for now lets return to what other commentators have to say about the Panopticon.

Reed provides some interesting comments:

"She consistently maintains that the vastly enhanced potential for control and disembodying that panoptican power makes available to employers and managers does not necessarily guarantee their success - their actual implementation and organisational consequences are unavoidably the subject of unpredictable socio-political conflict and struggle. The information systems constitutive of 'panoptican power' can 'alter many of the classic contingencies of the superior-subordinate relationship, providing certain information about subordinates' behaviour while eliminating the necessity of face-to-face engagement; they can transmit the presence of the omniscient observer and so induce compliance without the messy conflict-prone exertions of reciprocal relations" (Reed p.275).

The possibility that the managers novel attempts at increased control can, and is, thwarted are discussed:

"Unilateral techniques of control tend to evoke techniques of defence from subordinates who resent their own involuntary display. While these defensive measures can be thwarted, they can also contaminate the validity of data. Even more important, this battle of techniques of control versus techniques of defence signals the erosion of reciprocal relations as information becomes the field on which latent antagonisms are let loose . . . .The electronic text can insulate managers from the felt realities of their workplace that they will no longer have available the means with which to rekindle reciprocities if they should want to. Paradoxically, that very insularity increases the vulnerability of the text to contamination while it simultaneously heightens the requirements for valid objective data. Thus insulated, managers often collude in ignoring the even more slender relationship between their data and the organisational realities they are meant to reflect." (Zuboff quoted in Reed p.275)
Reflecting on how the above antagonisms may effect future organisations Reed states:

"The new control possibilities released by greatly enhanced technological and organisational power can restructure the 'rules of the political game' in which the major players are involved (p.275)...."

"None of the organisations that Zuboff researched had succeeded in implementing the 'information panoptican' to its full theoretical or technical potential."

**Exercise:**

Why do you think Zuboff failed to find any organisation that had fully implemented the 'Information panoptican'?

One aspect of the Panopticon that is often forgotten is the idea of isolation, for "Bentham believed that the nature of the human person can be adequately described without mention of social relationships. To begin with, the idea of 'relation' is but a 'fictitious entity', though necessary for 'convenience of discourse.' And, more specifically, he remarks that 'the community is a fictitious body,' and it is but 'the sum of the interests of the several members who compose it'. Thus, the extension of the term 'individual' is, in the main, no greater and no less than the biological entity. Bentham's view, then, is that the individual--the basic unit of the social sphere--is an 'atom' and there is no 'self' or 'individual' greater than the human individual. A person's relations with others--even if important--are not essential and describe nothing that is, strictly speaking, necessary to its being what it is." Taken from [http://www.utm.edu/research/iep/b/bentham.htm](http://www.utm.edu/research/iep/b/bentham.htm). He is therefore very much in opposition to those who were to come latter and suggest than interaction was an essential ingredient as to what defines self.

He suggested that his approach could be used in a number of settings including education and Hassard and Rowlinson 2002 provide details of how is approach was adopted in Joseph Lancaster's Monitorial Schools in the UK in the nineteenth century. Here are two quotes from the paper:

"Their paid monitors were under stricter discipline, more docile, better instructed, more skilful; and the whole organization of the school was consequently better ordered, and the instruction more exact and efficient" (Kay-Shuttleworth 1862: 106, describing a visit to a British School in Manchester in 1834 Quoted In Organization vol 9 issue 4 November 2002).

"Punctuality was...an essential in the monitorial schools whose structure had echoes of the developing production lines in the new factories. Not surprisingly Jeremy Bentham and the Utilitarians were keen advocates of the monitorial system" (Taylor 1996: 105-106 Quoted In Organization vol 9 issue 4 November 2002).

Returning to Zuboff, he concludes that new alternative strategies of organisational structure will evolve and importantly these strategies will be dependent upon the following for their success:

"The viability and success of these alternative strategies, ... will largely depend on the development of new ideological contexts and political skills in which the 'God' of bureaucratic rationalisation and control can be rejected for visions and practices of socio-technical transformations that resonate with the values and interests of 'high-trust' relations in work and society." (quoted by Reed p.276).

Zuboff appears here to be talking of a post Modernist world, similar to that described by some of the writers concerned with the Electronic Global Village. These issues are considered in more depth in another document concerned with social issues of the Internet. The subsection below provides a list of links about Bentham for those of you who are interested in him.
2.1 Web links

The original picture of the Panopticon:
http://www.ucl.ac.uk/Bentham-Project/Faqs/index.htm

To discover where panopticons were built see:
http://www.ucl.ac.uk/Bentham-Project/Faqs/fpanwher.htm

Another picture of a Panopticon is at:

or:

For a bit of light relief, look at the contemporary Panopticon in Manchester, UK:
http://www.postcardsfromprison.com/prison.htm#prisons

Michel Foucault: The Missing Pictures from Discipline & Punish
http://monarch.gsu.edu/jcrampton/foucault/foucault_dp.html

For a detailed article about the Panopticon see:
http://www.rochester.edu/College/FS/Publications/Lyon.html

The virtual Panopticon
http://is.gseis.ucla.edu/impact/f96/Projects/dengberg/

The original detailed specification by Bentham including use in hospitals and mad houses:
http://cartome.org/panopticon1.htm

Jeremy Bentham's requested in his will to have his body on display you can see it at:
http://www.cpm.ll.ehime-u.ac.jp/AkamacHomePage/Akamac_E-text_Links/Bentham.html

There is also a Jeremy Bentham project at University College London:
http://www.ucl.ac.uk/Bentham-Project/

For a list of Jeremy Bentham websites see:

Details of manuscripts and another pictures of Panopticon can be found at:
http://www-server.bcc.ac.uk/UCL-Info/Divisions/Library/special-coll/bentham.htm

Additional hyperlinks taken from Britannica.com:

http://www.utm.edu/research/iep/b/bentham.htm

University of Tennessee at Martin

Entry from the Internet Encyclopedia of Philosophy. After a discussion of Bentham's life and times, this entry treats his method, view of human nature, moral philosophy, and political philosophy. It also includes a bibliography of his works and a select bibliography of secondary sources.

The Pioneers: The Earliest Writers in English on Homosexuality
Summaries of books and articles on homosexuality dating from the 1700s. Includes the full text of Jeremy Bentham's "Offences Against One's Self: Paederasty" (c. 1785).
3. Technological determinism

A large amount of work has been undertaken to assert if technological innovation results in the development of a market or if its' development is due to a market need in the first place. Freeman 1987 et al provides a overview of the research in the first chapter of her book. The main findings would appear to be that the causal direction is dependent upon the particular technology and when it happens. One of the most interesting discussions in the chapter relates to the early development of the computer:

"the general view prior to 1950 was that there was no commercial demand for computers. Thomas J Watson Senior, with experience dating from at least 1928, was as well acquainted with both business needs and the capabilities of advanced competitive devices as any business leader. He felt that the one SSEC machine which was on display at IBM's New York offices 'could solve all the scientific problems in the world involving scientific calculations'. He saw no commercial possibilities. This view, moreover, persisted even though some private firms that were potential users of computers - the major life insurance companies, telecommunications providers, aircraft manufacturers and others were reasonably informed about the emerging technology. A broad business need was not apparent." [Freeman p.10 quoting Katz and Phillips 1981)

Freeman continues:

"Even latter, after IBM had produced a small batch of computers for the US Government during the Korean war, the Product Planning and Sales Department forecast no civil market for the model 650 computer. Against their opposition the Applied Science Group persuaded T. J. Watson Junior (who had taken over) to back the 650 model and forecast a sale of 200. In fact, 1800 machines were sold." [Freeman p.11]

The bulk of the chapter presents an increasingly complex picture to explain the trends in technological development. The last section has some interesting things to say about large organisations and technological development:

"Perez (1983) has suggested the big boom periods of expansion occur when there is a 'good match' between a new techno-economic 'paradigm' or 'style' and the socio-institutional climate. Depressions, in her view, represent periods of mis-match between the emerging new paradigms (already quite well advanced during a previous long wave of expansion) and the institutional framework. The widespread generalisation of the new paradigms, not only in the 'leading' branches of the upswing[?] but also in many other branches of the economy, is possible only after a period of adaptation of many social institutions to the requirements of the new technology. Whereas technological change is often very rapid, there is usually a great deal of inertia in social institutions, buttressed by the political power of established interest groups, as well as by slow response times of many individuals and groups." [Freeman p16]

Exercise:

How relevant do you think the above quote is to your organisation?
4. Managerial strategies

Child 1987 mentions four managerial strategies that are facilitated by technology:

- Virtual elimination of direct labour
- Spread of contracting
- Dissolution of traditional job or skill demarcations - 'polyvalence'
- Degradation of jobs by de-skilling.

Exercise:
Can you think of any examples in the health system where new technology has been introduced for any of the above covert or overt reasons?

He also lists the most common reasons for introducing new technologies based upon case study and survey analysis:

- Reducing operating costs and improving efficiency
- Increasing flexibility
- Raising the quality and consistency of production
- Improving control over operations

Electronic Point of Sale Systems (EPOS) found in most shops are given as good examples of a technological innovation which fulfils the above criteria. Related to the discussion of suitability for technological innovation is that of task uncertainty and complexity. This will be discussed in a subsequent section.

Exercise:
Suggest how the above criteria might be translated into a health care situation?
5. Freedom of Information and the Data Protection Act (DPA)

The Data Protection Act (DPA) in the UK is often cited as a complex powerful act when in contrast it has been described as:

"...Woolly, ambiguous and formless. The Act's supervisory body, the Data Protection Registry, is small, weak, burdened with some excessive regulation, constrained from entering too few real danger areas, and bereft of necessary powers of investigation, inspection and surveillance. Were the registrar and register now to disappear in a sea of paper, never to be seen or heard of again in Whitehall, the mandarins might well exchange thin, reserved smiles over a morning's sherry, and reflect quietly that data protection was less of an impediment to efficient public administration than first they had feared. This is how the British establishment had always seen off and neutralised irritating civil rights reforms, they would recall in their memoirs." [p144 Campbell & Connor].

The above quote might be considered to be rather jaundiced given that Campbell was a writer for the New statesman. However, most of the above has more than a grain of truth in it. A few salient points will be considered below.

The original act precluded a host of databanks from its jurisdiction including, payroll, accountancy data and 'All government activities' including; police, immigration and national-security activity. This means that any minister who wishes to deem any data the property of the 'government' in effect does not then require the data to be registered, or even acknowledged!

The BMA where one of the most critical professional bodies concerning the act:

"The BMA described it as 'a load of holes jointed together'. The major features criticised were the total exclusion of manual records, the vaguely drafted definitions and terms of reference, and above all the numerous and very wide spread exemptions" [p.138, Campbell & Connor].

The minuscule size of the original exercise can be demonstrated by considering the history of the organisation:

"The Data protection Act received the Royal Assent in July 1984. Mr Eric Howe, the Deputy Director of the National Computing Centre (NCC) in Manchester and chair of the National Computer User's Forum, was selected as the first Data Protection Registrar, at a salary of £35,000 a year - equivalent to a Deputy Secretary in the civil service. It took less than a year for him to discover that the home office's concept of fewer than 20 staff and a diminishing workload was an hilarious underestimate. In August 1985, the Registry was given an establishment of nearly 50 staff, with a starting budget of 1.2 million." [p.140]

Along with the development of the registry came registration and dissemination:

"The initial registration period ended on 11 May 1986. It is now an offence to operate a databank holding personal information unless you have registered. [In 1989] ...The register, itself stored on a computer by the Datasolve bureau, at a cost of about £2.5 million, will be published via libraries or Viewdata (Prestel) services."
Importantly the DPA registrar had and still has not authority to investigate 'illegal' databases unless an individual who believes data may be collected about themselves makes a formal complaint, in this sense the organisation is purely reactive rather than proactive as in the case of most departments (e.g. the copyrights department).

Over the years the DPA has evolved in terms of implementation, each University now having a DPA representative, but little has changed in terms of power or philosophy. From a medical viewpoint the strategic development of an NHS wide Network, which is a core component to the IT strategy (developed by the IMG at the DoH) has re-awakened fears of data confidentiality. A widely quoted report by Ross Anderson (Anderson 1996) considers a far wider range of implications presented by the NHS network than those considered by the DPA:

"The basic ethical principle, as stated by both the GMC and the EU, is that the patient must consent to data sharing. Confidentiality is the privilege of the patient, so only he may waive it [DGMW94]; and the consent must be informed, voluntary and competent [Som93]. Thus, for example, patients must be made aware that information may be shared between members of a care tam, 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 [DGMW94]. There is a 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." [Mac94]. Bold and italics added by me.

Ross Anderson also points a direct finger at the 'need-to-know' issue:

"The BMA does not accept that 'need-to-know' is an acceptable basis for access control decision. As the EU and GMC documents make clear, it is the patient consent that matters. The concept of 'need-to-know' implies and encourages the surreptitious erosion of the patient's privilege for the sake of administrative convenience. In any case, needs do not confer rights: the police's need to know whether a suspect is telling the truth does not give them a right to torture him. It is also useful to bear in mind empirical surveys of patient attitudes that show strong resistance to the sharing of personal health information with NHS administrators, social workers and government statisticians [Haw95]."

Clearly there is a tension between the BMA and the DoH and actually the tension is mounting as can be seen from a recent article by Ross Anderson entitled 'An update on the BMA Security Policy'. Quoting from the article:

"We were not to know it at the time, but the NHS Executive had projects underway to build systems that are in serious conflict with medical ethics as understood by both doctors [31] [32] and patients [17] [36] [59]. If security rules are adopted that enforce this traditional view, then these systems will require significant changes (which we discuss below)."

[Source: http://www.cl.cam.ac.uk/users/rja14/bmaupdate/node2.html]

**Exercise:**

1 Information Management Group (the IT policy department of the NHS ME). Replaced in 1998 by the NHS Information Authority (NHSIA)
What 'professional' methods of control do the medical profession use. Do you feel they are all legitimate?

More recently (1998) the DPA has been amended, the changes largely stemming from the EU Directive 95/46/EC.

* Fulfilling the provisions of the Act will mean extensive changes to existing systems in many cases. Systems that hitherto, have been outside data protection law. The Act does not differentiate computer or other technology: PCs are subject to the law as are mainframe, closed circuit television and other automated processing systems. Outputs from such systems are within its domain.

The DPA1998 defines personal data very broadly and the definition extends to any data that can be linked to a living human being. Data Protection law now applies to certain types of manual records. The DPA1998 introduces the concept of sensitive data and extends the data subject's rights of access to data and the control of its use. The Act entitles the data subject to compensation where a data controller is in breach of the Act's terms and principles. A data subject can apply to the County Court for inaccurate data to be corrected, erased, or blocked. Under the DPA1998 all managers in an organisation are liable for breaches of the Act.

Use of personal data must be with the consent of the data subject. Although consent is deemed to be given under circumstances that the data subject should be aware that the information he supplies will be processed within the meaning of the DPA. For example, an application for an Electricity supply means that the data subject has consented for the data to be used for billing him and supporting the supply of power to his address.

The Act, as at 12 July 1999, still remains to be fully implemented awaiting Statutory Instruments. The recently published Freedom of Information Bill (FOI1999) has repealed some of the DPA1998 provisions as they affect government bodies. Public bodies will have to comply with both the DPA1998 and the FOI1999 when enacted.

[John Watt at http://members.aol.com/ASRSvcs/DPA1998.htm]

According to the government site: http://www.open.gov.uk/dpr/eurotalk.htm The Government has announced that the Act will be brought into force on the 1st March 2000.


Returning to Ross Anderson's concern about the 'need to know' policy it is interesting to note that it has been accepted by the Caldicott committee's report.

Concerning the Internet Home secretary Jack Straw has outlined plans to update the communications act (July 1998) which will allow e-mail tapping. See http://www.homeoffice.gov.uk/oicd/ioca.pdf.

The above section could do with updating anyone reading this who would like to contribute to the content please e-mail me.
5.1 Caldicott

In December 1997 The Department of Health Published the Caldicott Committee 'Report on the Review of Patient-Identifiable Information'. The executive summary contains 16 recommendations and 6 general principles. These are given below:

Principles concerning patient-identifiable information:

1. Justify its purpose
2. Don’t use patient-identifiable information unless it is absolutely necessary
3. Use the minimum necessary patient-identifiable information
4. Access to patient-identifiable information should be on a strict need-to-know basis
5. Everyone with access to patient-identifiable information should be aware of their responsibilities
6. Understand and comply with the law [i.e. develop Caldicott guardians]

Recommendations:

Recommendation 1: Every flow of information, current or proposed, should be tested against these principles as a matter of course. Continuing flows should be re-tested regularly and routinely.

Recommendation 2: ..A programme of work, led by the NHS executive, be established to reinforce confidentiality and IM&T security requirements amongst all staff within the NHS.

Recommendation 3: A senior person should be nominated in each NHS organisation . To act as a "guardian".

Recommendation 4: Guidance must be provided for those individuals/bodies responsible for approving uses of patient-identifiable information (e.g. the "guardian" or research ethics committees) to enable them to critically appraise new proposals and continuing practice.

Recommendation 5: We wish to see the Department and the NHS, along with partner organisations, jointly identify the key areas in which protocols are required and prepare and publish good practice frameworks for local adoption in these areas.

Recommendation 6: ..., each NHS and non-NHS organisation clearly establishes and communicates to partner organisations who is responsible for monitoring the sharing and transfer of information within the local agreed protocol.

Recommendation 7: The possibility of an accreditation system, which would recognise those organisations which follow good practice with respect to confidentiality, should be explored by the Department of Health in partnership with interested groups.

Recommendation 8: The new NHS number should replace patient-identifiable data, as soon as practically possible, in every data flow where there is a need to distinguish between individuals but where there is no immediate corresponding need to identify those individuals. Continued use of additional patient-identifiable data items for other purposes must be robustly justified. The Department of Health should urgently pilot the use of NHS number as the main identifier, e.g. in contracting flows.

Recommendation 9: The NHS Executive in partnership with professional bodies, should develop strict protocols to define which individuals are authorised to gain access to patient identity (e.g. where the new NHS number is the main identifier, through use of the NHS Number Tracing Service or through access to administrative or other population registers), and under what circumstances access should be authorised.

Recommendation 10: Where particularly sensitive information is to be transferred, the use of privacy enhancing technologies (e.g. encrypting the NHS number) must be urgently explored.

Recommendation 11: ..that the appropriate trade and professional associations are encouraged to raise awareness amongst their members, and that institutions providing training in healthcare Informatics are encouraged to include privacy enhancing technologies as part of those training programmes.

Recommendation 12: The internal structure, and administration, of databases should reflect the principles developed in this report, e.g. separating patient-identifying details from event,
treatment, or condition information with linkage possible only under specific and controlled circumstances. Whilst it is recognised that there may be practical barriers to restructuring existing databases, the practicalities of doing so should be explored.

**Recommendation 13:** The new NHS number should replace the patient’s name on Items of Service Claims made by General Practitioners as soon as is practically possible. The software used by all General Practitioners, the Dental Practice Board and Health Authorities should be reviewed to determine the resource consequences of specification changes which would be required to support changes in practice as recommended in this report.

**Recommendation 14:** The design of new systems for the electronic transfer of prescription data should incorporate the principles developed in this report.

**Recommendation 15:** Negotiations on pay and conditions for GPs should have regard to the desirability of avoiding systems of payment which require patient-identifying details to be transmitted.

**Recommendation 16:** The practicalities of piloting new procedures for claims and payments which do not require patient-identifiable information to be transferred should be urgently considered, e.g. batched claims with details held in general practice for audit purposes.

It is interesting to note that recommendation 2 also stipulates that the programme of work should include:

"ensuring that, in all cases where access to patient-identifiable information held electronically is necessary, computer systems must adhere to the requirements set out in the NHS Executive's IM&T Security Manual, implement appropriate security controls and provide audit trails of access to such information."

If one interprets the above "all cases" to include research databases, audit data and such like I feel that adherence to the above recommendations, particularly that of a audit trail, would be impossible. While the Caldicott recommendations are largely sensible and achievable I feel that in this instance it is just not so.

**Exercise:**

Within your organisation do you feel all the above recommendations are necessary? Also are they all achievable?

Ross Anderson, a security expert from Cambridge University, has voiced many reservations concerning the Caldicott recommendations. Amongst which are those concerning the proposal for a National NHS number tracing service. The reasons for his concern are:

1. "The experience with large databases to which many people have access (e.g. criminal records, vehicle registrations, bank statements) is that access to them is corruptly sold by insiders, and this corruption is extremely hard to prevent.

   Even where Caldicott-style controls are attempted (e.g. make all a police station's criminal record enquires go through the custody sergeant) it doesn't work (so many people call the sergeant on the phone or the radio for an enquiry that proper records can't be kept).

2. computer security awareness and discipline is very much poorer in the NHS than the police.

   I have found just yesterday that at a local hospital, people routinely log on using the passwords of junior doctors who moved on six months ago. Also, there are no mechanisms to perform regular penetration testing, and there's no system of security clearances for non-clinical staff.

3. The NHS Tracing Service database will be the only database of all adults and children in the UK - the NI database is incomplete as it doesn't include children and many addresses are out of date; the DVLA ditto and omits recent immigrants; the electoral register is similar but doesn't even have your date of birth. Other government departments will ask for and get access - the obvious ones are the police, customs, MI5, the immigration and naturalisation service, the social security fraud squad, the child support agency, and the register of sex
4. It will be immensely valuable to debt collectors, solicitors seeking to issue writs and anybody else who needs to trace people (from the Iranian secret police to the IRA and the Mafia). So there will be a huge incentive for private eyes to bribe NHS staff and get access. The number of people with unlawful access will also snowball.

…I predict that once the public understands this a lot of people will either give false names or dates of birth; others will simply avoid seeking treatment. These will not just include the ‘undeserving’ such as delinquent dads…. But also ‘deserving’ cases such as battered women and people on the witness protection programmes, and ‘borderline’ cases such as sex offenders with psychiatric problems.”

[Taken from a reply to GP-UK@mailbase.ac.uk Monday, 29th June 1998 14:25:34 hrs.]

The Information for Health document also clearly has concerns over this aspect of Caldicott:

"Protocols to ensure use of the NHS Number Strategic Tracing Service is strictly based on authorised access for authorised purposes will be agreed as a matter of urgency" (p53)

6. Clinical Governance

The NHS Executive document - Information for Health (NHS E 1998) defines Clinical Governance to be:

A national framework through which NHS organisations are accountable for continuously improving the quality and clinical effectiveness of their services. (p117)

In other words clinical governance is both a management structure and a process. Many have rightly said (see RCGP 1999 p2) that this is just an example of re-packaging of several well established concepts. What it does do is repackage these concepts into something that provides an overall framework of monitoring and standard setting from the individual to the national level. It could be suggested that Clinical Governance allows the Panoptican in through the back door? The sections below discuss this.

6.1 The structure

The Primary Care Group (PCG) came into being in April 1999, initially as advisors to their Health Authority on commissioning of services, or taking devolved responsibility for managing the budget for healthcare in their area. A "leader for clinical governance" was appointed who was also a member of the PCG (RCGP 1999, p1).

Within the Hospital environment it is felt that the structure will be largely assimilated into that of clinical audit.
6.2 The process

Information for Health (NHS E 1998) states that:

"It .. requires a culture amongst clinical staff where the obligation on individuals to assess personal performance continually is accepted as a natural and important element of being a professional." (p76)

This once again reflects the clinical audit framework. However clinical audit tends to be at a low level, often discussing individual patients whereas in Clinical governance the emphasis is on comparative data, Information for Heath (p68) recommending that information be drawn from:

Local audit data
National comparative data
Local care pathways and clinical protocols
National best practice guidelines
National Institute for Clinical Excellence (NICE) evidence
International research evidence

Clinical Governance therefore encompasses audit, guideline /pathway development, standards setting and a host of other activities. It is this clever juxtapositioning of these local and national activities, which are uncomfortable bedfellows, that is new and possibly dangerous. The need for 'national comparative data' is assimilated within the professionally more worthy activity of local audit.

Within the Primary care context the RCGP (RCPG 1999 p6) suggests that the Clinical Governance process should concentrate on three aspects:

Protecting patients:
- Registration of professional qualifications (and perhaps in time revalidation of the registration)
- Identifying unacceptable variations in care and areas in need of improvement
- Managing and minimising poor performance in colleagues
- Risk management

Developing people:
- Continuing Professional Development (CPD) or lifelong learning
- Development and implementation of guidelines and protocols for "best practice"
- Personal accreditation
- Recognising and celebrating success

Developing teams and systems:
- Learning from what other teams do well
- Clinical Audit
- Develop and implementation of guidelines and protocols for "best practice"
- Recognising and celebrating success
- Evidence based clinical practice
- Improving cost effectiveness
- Listening to the views of patients and carers
- Practice accreditation
- Through all these, promoting accountability and transparency
Once Clinical Governance is fully operational the leader for clinical governance will be expected to offer evidence in the following areas (RCGP 1999, p7):

- An effective system for monitoring the performance of teams and individuals
- An effective system of risk management
- An effective system for lifelong learning for individuals and teams
- An effective system for implementing and monitoring evidence based guidelines and National Service Frameworks
- An effective system for accrediting teams and individuals

From the above it can be seen that certain aspects of Clinical governance attempt to reduce task uncertainty (‘risk reduction’) and choice (guidelines etc) thereby reducing task complexity. This has important implications which are discussed below.

7. Task Uncertainty and Complexity

The gradual erosion of confidentiality be it patient or health care professional, due to the development of the ‘panoptican’ vision, appears relatively limited in the health care arena due to the high level of uncertainty and complexity inherent therein. Child discusses these characteristics further:

"There is some consensus among organisational theorists that the most significant task dimensions for an understanding of how work is organised are those relating to uncertainty and complexity (cf. Perrow, 1970, Van de Ven and Ferry 1980). The number of exceptions encountered in performing the task and its general variability, a lack of clarity about what is required and about cause-effect relationships are all factors contributing to uncertainty. Complexity is increased by factors such as the amount of relevant information to be absorbed in carrying out the task, the number of steps involved, and the number of contributions required from different sources. A third relevant dimension is the cost of making an error, whether this falls primarily on property or on a person."

Exercise:

Considering the two dimensions, of complexity and uncertainty. What would you consider to be those clinical tasks which are relatively simple, if any, and those which are highly complex.

Which of the above roles identified by yourself do you think most clearly defines you as a professional.

How do you cope with uncertainty in the clinical situation?
"An analysis of the introduction of new technology into medicine, banking and retailing conducted by the writer and colleagues (Child et al 1984) concluded that task uncertainty and the cost of error were particularly significant for enabling service providers to preserve the integrity of their jobs. New technologies will normally have a superiority in receiving, storing and providing rapid access to complex data, so long as these are in a structured form. Moreover, tasks involving uncertainty and risk require the exercise of judgement: the best way of carrying them out is not transparent. This 'indeterminancy' has a considerable ideological potential for the defence of the worker's control over the labour process, as professional workers in particular have demonstrated (Jamous and Peloille 1970). **In short, the greater the uncertainty and risk in tasks to be performed, the less likely are strategies of labour elimination or job degradation to be adopted.**" [p.93]

**Exercise:**

Job degradation by nurse practitioners is already happening, how is this being facilitated by computers. Are there any limitations?

Uncertainty and complexity are key characteristics of most clinical situations which this section has just touched upon. Other chapters on social issues will investigate this issue in greater depth specifically looking at the 'clinical method'.

### 7.1 Summary

This short introduction to some of the social issues surrounding health Informatics has presented a few of the inherent social problems associated with new technologies or information systems. The 'panopticon' concept was introduced and how this might relate to certain aspects of Clinical Governance suggested. The inherent uncertainty and complexity of the clinical situation was discussed indicating how these characteristics have tended so far to protect the professionals from the effects of the panoptican.

The history of the data protection act was discussed alongside the BMAs initial response and other more general confidentiality issues. The next document will concentrate on these social issues regarding Informatics in the clinical process.
8. References

Anderson Ross 1996 Security in clinical Information Systems BMA publications
Anderson Ross 1998 NHS Tracing Service. Reply to GP-UK@mailbase.ac.uk Monday, 29th June 1998 14:25:34 hrs
Dreufus Hubert I 1993 What computers still can't do: A critique of artificial Reason. The MIT press London
Finnegan R Slalman G Thompson K 1987 Information Technology: Social Issues A Reader Open University/ Hodder & Stoughton
Foucault Micheal 1975 Discipline and Punish Penguin Books
Reed Micheal I 1992 The sociology of organisations. Harvester Wheatsheaf
Royal College of General Practitioners 1999 Clinical Governance: Practical Advice for Primary Care in England and Wales.
Ryczynski Witold Taming the tiger: The struggle to control technology. Penguin books
Watt, John 1999 The 1998 DPA http://members.aol.com/ASRSvcs/DPA1998.htm ASR Services Ltd, PO Box 6943, Dundee, DD3 0YG. Tel. 01382 320729, Fax. 01382 320719. Email: asr-svcs@dircon.co.uk

************************************************************************

Document details

Original 26/08/1999
Revised: 17/06/2003 18:29