Current **United Kingdom**/European Union Law Related to Privacy & Health Information

Peter Singleton, MBA* & Don E. Detmer, MD**

*Cambridge Health Informatics

**American Medical Informatics Association; University of Virginia

NCVHS Hearing

June 7, 2005

This presentation draws heavily upon a presentation given by

Peter Singleton to the

U.K. Medical Research Council Workshop

July 1, 2004

Messages & Differences from USA

- Biggest difference - Universal state provision
  - Approx. 10 plus % private insurance
- Situation in flux due to recent UK & EU laws
- Medical community feels current policies damage biomedical research
- Compared to USA
  - Electronic records are less of the issue
  - Unique Health Identifiers is not an issue
  - Much less media intensity around privacy
- Mandatory Citizen ID Cards is an public issue

Outline

- Current General Status
- Ethical Background
- Legal Background
- Issues of Consent
- Anonymisation
- Discussion

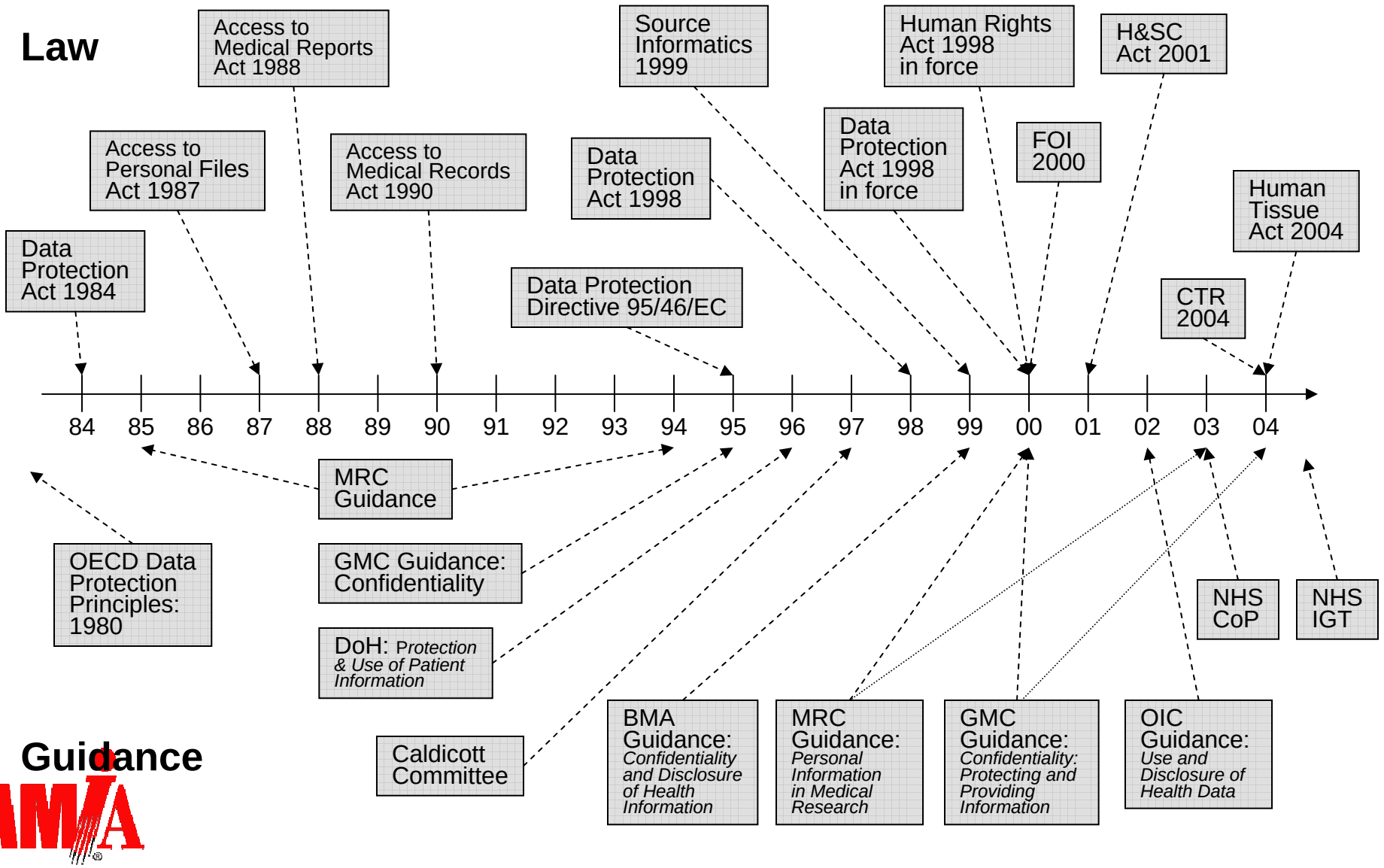
NHS Information Governance Model - **HORUS**

- **H**olding – should you have it?
- **O**btaining – did you get it properly?
- **R**ecording – is it accurate/meaningful?
- **U**sing – what are proper purposes?
- **S**haring – who else can/should have it?

Essentially Parallels Ethics

- Medical principles:
  - Benevolence – do good
  - Non-maleficence – avoid doing harm
  - Autonomy – respect for individual
  - Justice – equity between all
- Balancing protecting individual against society's needs, e.g., public safety, public health
- Depends on circumstances, so difficult to codify

Confidentiality Issues Timeline



U.K. Legal Background

- Common Law of Confidentiality
- OECD Principles
  - –Organisation for Economic Co-operation & Development
- Data Protection Act 1984
- Access to Medical Reports Act
- Access to Health Records Act 1990
- EU Directive 1995
- Data Protection Act 1998
- Human Rights Act 1998
- Health & Social Care Act 2001

Common Law of Confidentiality

- Not written in statute
- Based on case law
- Can seek redress for damages
  viz. might be sued, not arrested!
- Very few cases relevant to medical records – most clear breaches of duty
- *Regina* vs. DoH ex parte *Source Informatics (effectively allowed use of anonymized data)*

General regulation

- Data Protection Act 1998 (UK version of EU Directive) – proper holding & use of information; paper or digital
- Human Rights Act 1998 – right to ‘private life’
- Freedom of Information Act 2000
- EU Clinical Trials Directive 2001: Clinical Trials Regulations 2004
- Human Tissue Act 2004

General Regulation

- Human Rights Act 1998 –
  - Article 8 - respect to a ‘private life’
  - First hint towards ‘a right to privacy’ in UK
  - Interpretation not yet clear – will depend of courts
    - Non-intrusion vs. restriction of external information

Data Protection Act 1998

- UK Version of EU Directive
- Applied equally to paper and electronic media
- Extended requirements to ‘processing’ not just ‘notification’
- Set definitions & principles
- via Schedules 2 & 3, consent exemption for ‘medical purposes’, includes research

Health & Social Care Act 2001

- Tricky passage through Parliament
- Key area is Section 60 - allows certain data uses to be exempted from consent
- Created Patient Information Advisory Group (PIAG) to advise Secretary of State
- Applies only in England & Wales

Section 60 of H&SC Act

- Applications working through PIAG: some specific projects; some ‘class’ applications
- Only few to start with; major backlog due soon
- Broad principles likely to be developed as more cases come through, but may not lead to clear ‘answer’

PIAG Principles

- Ultimately must have **consent** or **anonymise** the data
- Purpose must be beneficial & proportionate
- Must have effective security, confidentiality, & data retention & disposal policies in force

Variety of Sanctions

- DPA 1998
  - Correction of errors
  - Possible confiscation of data
- H&SC 2001
- Common Law of Confidence
  - Could be sued for damages (if any)

Other Relevant Statutes

- Laws mandating data-sharing
  - e.g. Communicable Diseases Act
- Laws permitting data-sharing
  - e.g. Health & Social Care Act 2001 – S60; Prevention of Terrorism, Road Traffic Acts
- Laws prohibiting data-sharing
  - e.g. Venereal Diseases Act, Human Fertilisation and Embryology Act, Abortion Act
- Laws on data subject access to data
  - Data Protection Act 1998 – subject access requests; Access to Medical Records 1990

Relevant Regulations

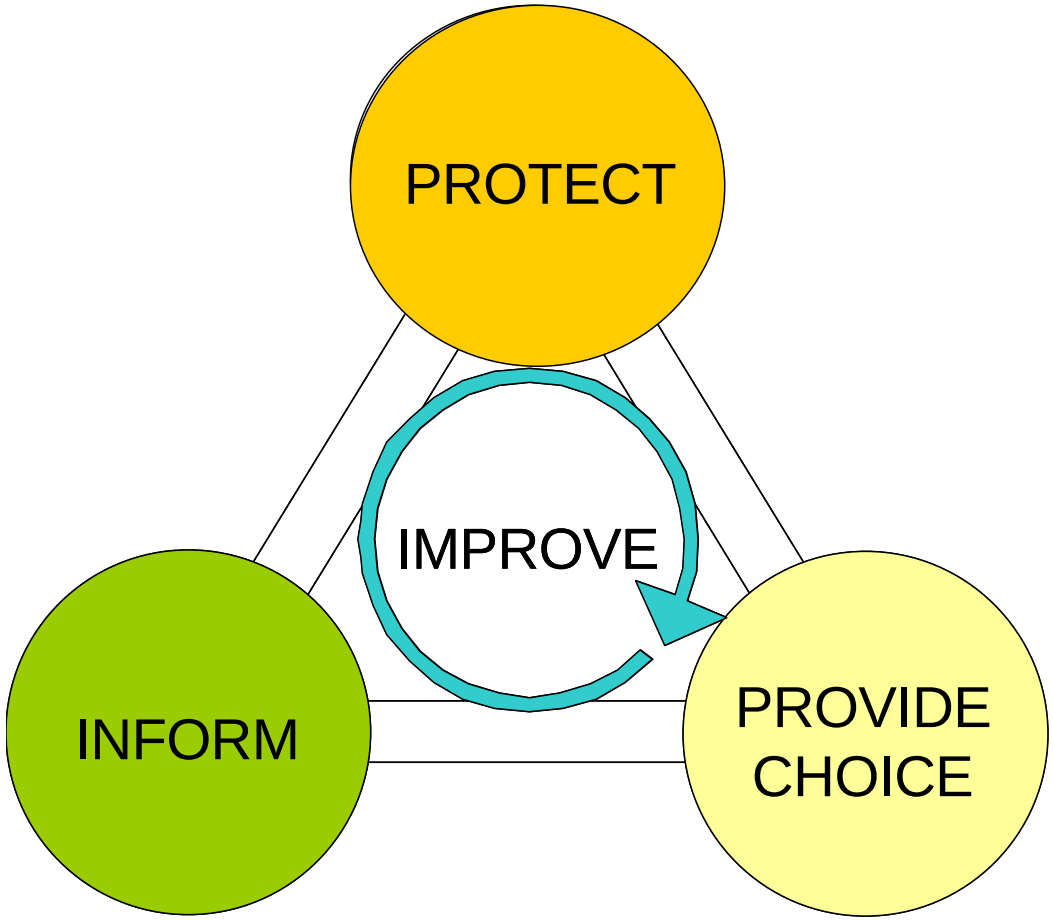
- NHS Information Governance
- NHS Confidentiality Code of Practice
- Research Ethics Committees
- OIC Guidance (2002)
- GMC Guidelines (Updated April 2004)
- MRC Guidelines (updated 2003)
- BMA Guidance (1999)
- PIAG Principles – see web references

Information Governance in Practice

- Seeks to bring together a number of related initiatives:

  Data Protection; Caldicott; Security; Data Quality; Consent/Confidentiality; Freedom of Information; Health Records Management
- IG Toolkit currently used to assess Acute Trusts – will be extended to PCTs, MHTs, GPs, etc. in 2004/5
- Reflected in Healthcare Commission ratings
- Inactive at present under National Programme

Confidentiality Code of Practice



Anonymisation

- DPA 1998 covers:
  'data which relate to a living individual who can be identified- (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller'
  viz. any data about a living person who could potentially be identified
- Source Informatics case established that 'anonymised' data does not breach confidentiality

Thank you

detmer@amia.org

peter.singleton@chi-group.com

Miscellaneous Addenda

- Issues of Consent
- Consent in Different Contexts
- Consent in Clinical Trials
- Areas of Uncertainty
- Readings
- Related Websites
- Source Informatics Case
- Privacy v. Security v. Confidentiality

Issues of Consent

- ‘Imputed consent’ – if I were to ask you, I am sure you would consent
- ‘Implied consent’ – informed, but ‘silence signifies consent’ – ‘opt-out’
- ‘Express consent’ – only if agreed – does not have to be written, but must involve positive action – ‘opt-in’
- ‘Express written consent’ – to ensure standard form and evidence – may still be coerced, ill-informed, or misunderstood

Consent in different contexts

- Consent to examination or treatment
  - Must precede intervention
  - Consent to clinical trial is different context
  - Non-approved care protocols may be different (?)
- Consent to tissue or organ retention
  - Need may occur after intervention
- Consent to genetic testing
- Consent to sharing of information
- Consent to publication

Consent in Clinical Trials

… a person gives *informed consent* to take part, or that a subject is to take part, in a clinical trial **only if** his decision - (a) is given **freely** after that person is **informed** of the nature, significance, implications and risks of the trial; and (b) either -

- (i) is **evidenced in writing, dated and signed**, or otherwise marked, by that person so as to indicate his consent, or
- (ii) if the person is unable to sign or to mark a document so as to indicate his consent, is given orally in the presence of **at least one witness and recorded in writing**.

Areas of uncertainty

- What ‘consent’ is sufficient?
- When is a data-set ‘anonymised’?
- How ‘informed’ should patients and the public be?
- What to do about third-party data/family histories
- What is the balance between public good and individual risk?
- What does a researcher need to do to get it right?
- Research in mental health raises problems over consent where incapacitated
- Data retention – for specific study vs. ‘just in case’

Further Reading

- Ashcroft: *Ethical, Legal and Social Issues Facing the West London Database Project: A Review of the Literature*
- Singleton: *ERDIP N5 – Consent Study*
- O'Neill: *Autonomy and Trust in Bioethics*, CUP
- Lowrance: *Learning from Experience: Privacy and the Secondary Use of Data in Health Research*
- OIC: *Use and disclosure of health data*
- www.dh.gov.uk/assetRoot/04/06/92/54/04069254.pdf
- http://www.informationcommissioner.gov.uk/cms/DocumentUploads/webversion%204%2004.10.042.pdf

Related Websites

- www.nhsia.nhs.uk/infogov
- http://www.advisorybodies.doh.gov.uk/piag/
- www.nhsia.nhs.uk/infogov/pages/default.asp
- www.dataprotection.gov.**uk**/
- http://www.chi.nhs.uk/
- (www.dh.gov.uk/PolicyAndGuidance/HealthAndSocialCareTopics/Consent/ConsentGeneralInformation/fs/en)

Source Informatics case

Source Informatics Ltd requested access to anonymised data from patients' prescription forms. This information would be of great commercial value to pharmaceutical companies wishing to market their products more effectively because they could find out more about how their products were being used. Source Informatics wanted to create a database for this purpose, paying a small fee to the GPs and pharmacists for their trouble.

The Department of Health (DH) refused them access on the basis that it would be a 'breach of patients' confidentiality'. Source Informatics went to court but the judge ruled in favour of the DH.

On appeal, this decision was reversed. The Court of Appeal concluded that personal information can be used for public health research purposes providing that appropriate steps are taken to conceal the participants' identities.

Source Informatics case

SIMON BROWN LJ said that in a case like the present which involved personal confidences the concern of the law was to protect the confider's personal privacy. That alone was the right at issue. **The patient had no proprietorial claim to the prescription form or to the information it contained.** The patient could bestow or withhold his custom as he pleased. The pharmacist had no such right. He was by law bound to dispense to whoever presented a prescription. But that gave the patient no property in the information and no right to control its use provided only that his privacy was not put at risk. **Participation in the applicant's scheme by doctors and pharmacists would not expose them to any serious risk of successful breach of confidence proceedings by a patient.** If the Department of Health continued to view such schemes as operating against the public interest, then they must take further powers in the already heavily regulated area to control their effect. **The law of confidence must not be distorted for the purpose.**

Privacy vs Security vs Confidentiality

- Privacy – the right to keep private
  - Prevent use, sharing, retention of data
- Confidentiality – appropriate sharing
  - Protecting the person's interests
  - When to share; when not to share
- Security – the protection and assurance
  - Access controls/encryption
  - Disaster recovery/data integrity
- Libel & slander - untruths