ESRC Seminar Series: Big Data and Employee Well-Being

Principles of good data governance

Graeme Laurie

School of Law, University of Edinburgh

LiminalSpaces

wellcome trust Investigator

THE UNIVERSITY of EDINBURGH
Edinburgh Law School

Overview

- **The main RQ:** how might employees be ethically and lawfully monitored for the purposes of safeguarding employee well-being?
- Good information governance as essential to responsible regulation
- Principles-based Regulation (PBR) v Rules-based Regulation (RBR)
- Examples from ScottisH Informatics Programme (SHIP) and Scottish Medical Educational Research Consortium (SMERC)
- Law as *architecture* and *process*: what are we missing in-between?
- Some thoughts to inform a Good Governance Framework

Supported by wellcome trust

What is PBR (as opposed to RBR)?

- Principles are (normally) fundamental starting-points to guide deliberation and action
- Principles are not rules in the prescriptive sense of being action-determining (although…see next few slides)
- Principles reflect the values of an organisation or an initiative, ideally they are mutually agreed and co-produced
- Principles do not (normally) determine action – they help guide judgments and might be deployed in different ways in different contexts
- PBR can fosters governance behaviours that embrace the reality that subtle judgments about the value and risks of data linkage and use must often be made *within* existing legal frameworks.

Principles in law: the DPA and the DPD Eight Principles

- Principle 1 – **fair and lawful**
- Principle 2 – **purposes**
- Principle 3 – **adequacy**
- Principle 4 – **accuracy**
- Principle 5 – **retention**
- Principle 6 – **rights** (subject access request; damage or distress; preventing direct marketing; automated decision taking; correcting inaccurate personal data; compensation)
- Principle 7 – **security**
- Principle 8 – **international conditions for processing**

Towards a Principles-based Approach (PBA)

- Some principles are rules and some rules are principles
- More accurately: some principles are rule-like and some rules are principle-like
- Consider a *spectrum* of function:
  - Purely action-guiding **principles** sit at one end
  - Entirely action-determining **rules** sit at the opposite end
  - Hard law sits towards this latter end ("Regulation")
  - Sound ethical conduct (ideally) crosses the entire spectrum
  - "Good governance" requires legal compliance and sound ethics!

Supported by wellcome trust

Employer-employee data use: a framework

- **A compliance element** (DPA 1998, Human Rights 1998, Employment, Equality etc…)

- **A normative element** (which principles?, which objectives?, which actors?, which elements?, which limits?)

SHIP: legal and ethical challenges (2009-2013)

- **Main RQ:** How can we optimise the value for Scottish health and wealth by improved access to medical records for research purposes?
- Data Protection Act 1998, common law of confidentiality; human rights considerations
- A plethora of standards, policies, guidelines and decision-makers
- The challenge: translating law and ethics into practice
- What's the problem? Too many rules!
- What do we want? More rules!

SHIP: good governance framework (2009-2013)

Principles and best practices approach

- **Principles:** "… fundamental starting-points to guide deliberation and action. They reflect the values that underpin the SHIP project and its commitment both to promote the public interest and to protect individual interests."
- **Best practices:** "… examples of principles in action. These are instances of optimal governance and in that sense they are aspirational. As with principles, where instances of best practice are not or cannot be followed, clear justification should be offered."

SHIP: principles and best practices

Principles: 1. Public Interest

- Scientifically sound and ethically robust research is in the interest of protecting the health of the public.
- The rights of individuals should be respected with adequate privacy protection, while at the same time the benefits for all in the appropriate use of health data for research purposes should be recognised.
- Data sharing and use should be carried out under transparent controls and security processes, and the purposes and protection mechanisms should be communicated publicly and to oversight bodies/individuals with responsibility for data processing.
- The responsible use of health data should be a stated objective of all organisations adhering to this instrument.

Best Practice

- It is the data controller's responsibility to ensure the development of transparent policies that demonstrate their understanding of public interest and the basis upon which they will use and disclose health data; equally importantly this must include the protection mechanisms under which use will take place.

SHIP: principles & best practices - consent

Principles

- Personal data must not be used without consent unless absolutely necessary….
- The refusal of data subjects must be respected unconditionally.
- Where possible and practicable, individuals collecting data should adequately inform data subjects of all material issues relating to the storage and use of their data….
- Where obtaining consent is not possible/practicable, then (a) anonymisation of data should occur as soon as is reasonably practicable, and/or (b) authorisation from an appropriate oversight body/research ethics committee should be obtained.

Best Practices

- Consent procedures should be designed to obtain free and meaningful consent, that is, data subjects must be given sufficient information to make a decision that reflects their genuine wishes, must be given the opportunity to ask questions and have these answered, and must not be subject to coercive measures.
- Where there is the prospect of future use of data that is unknown at the time of consent, then data subjects should be informed of the broad purposes for which the data might be used. These purposes will delimit the appropriateness of any future use.
- Where consent is not to be obtained, the reasons for this must be clearly articulated and adequately justified.

Scottish Medical Education Research Consortium (2012-13)

- **Main RQ:** In what circumstances is it lawful and ethical to use medical students' training data and questionnaire responses for research to improve medical training and student support more generally?
- NHS Education Scotland and University of Dundee initiative
- Adopted PBR and Practices approach from SHIP
- A Framework for evaluation of existing IG approach (11 questions)
- Recommendations and best practices for moving forward

LiminalSpaces

Supported by wellcome trust

Scottish Medical Education Research Consortium (2012-13): recommendations

- Appropriate use of consent and re-consent;
- Understanding the alternatives to consent and thus the 'public interest' implicated by the work;
- Developing proportionate authorisation protocol to govern current and future uses of the research data;
- Using anonymisation as a tool to protect data subjects and facilitate SMERC research;
- Proportionate regulation of access to the research data;
- Using data sharing agreements to clarify existing and future data protection obligations;
- Protocols for maintaining the accuracy and quality of the research data;
- Determining appropriate data retention cycles; and
- Implementing robust security measures such as safe haven environments to protect the research data.

Top-down and bottom-up

"'We need ethical principles at a high level and this should permeate down to all levels - 'governance' is a management question in terms of having the right ethical attitudes at the top; and it is a cultural question, by ensuring that the attitude permeates every aspect of business operation and conduct."

Arjoon, Striking a Balance Between Rules and Principles-based Approaches for Effective Governance: A Risk-based Approach **(2006)**

Principles-based approach (PBA)

- PBA focuses on broad-based standards in preference to detailed rules, outcomes-based regulation and increasing senior management responsibility.

- PBA operates as an explicit statement of the core values and standards which underpin data sharing practices and arrangements. This can improve transparency, legitimacy and, hopefully, trust in systems that apply this approach;

- PBA provides decision-makers with a common frame of reference, values and a language with which to make decisions. This can facilitate engagement and mutual recognition of governance arrangements which can reduce undue overlap;

- PBA engages with the full range of governance tools to ensure that appropriate governance pathways are applied to each data use.

PBA: some caveats

- Indeterminancy (engagement over interpretation)
- Conflict and balance (risk assessment of values and objectives)
- Sanctions (principles must not become too ‘rule-like’)

Supported by wellcome trust

Law as process

“The more ‘rational’ a society seems in its parts, and in its rules, and in its rules about rules, the thicker the layer of formalism and ideological self-representation to be penetrated to find out what is really going on.”

Falk Moore, Law as Process (1978)

Relevant publications

- Scottish Informatics Programme (SHIP): http://www.scot-ship.ac.uk/
- N Sethi and G Laurie, 'Delivering Proportionate Governance in the Era of eHealth: Making Linkage and Privacy Work Together' (2013) 13(2-3) Medical Law International 168-204
- G Laurie and N Sethi, 'Towards Principles-Based Approaches to Governance of Health-Related Research Using Personal Data' (2013) European Journal of Risk Regulation 43-57

Thank you

Graeme.Laurie@ed.ac.uk
@GraemeLaurie

Supported by wellcome trust