eHealth Workshop
25-26 April 2013
Middlesex University
London, UK
http://goo.gl/tgDaf

Data Protection and Privacy – implications for eHealth

Peter Singleton

UCL/Cambridge Health Informatics

Abstract

This talk will consider the tensions between the benefits of eHealth, particularly ‘big data’, coordinated care, and ‘personalised medicine’ and the concerns and risks to individuals’ privacy.

These are particularly highlighted by the current passage of the draft EU Data Protection Regulation where privacy concerns, particularly over Internet data collection, may be dominating over ‘real-world’ scenarios, such as eHealth where the need is for greater use of medical data rather than less.

If the fundamental issues are not considered carefully then there is a real risk that we may allow theoretical risks to privacy to dominate over other rights (e.g. to health and safe healthcare).

Do we need to promote ‘good practice’ rather than create further individual ‘privacy rights’? Should we emphasise patient choice rather than legal ‘consent’? What are the implications for developments in eHealth and for healthcare?

Overview

- ‘Big Data’, ‘personalised medicine’ – what do they mean?
- Coordinated care – linking data across care providers – and with patient’s own experience
- What processing is part of good practice in healthcare delivery
- Draft Data Protection Regulation – promotes privacy
- Data Protection versus privacy, security & confidentiality
- Personal data and anonymisation – thinking about risks
- Explaining this to public, politicians, and lawyers

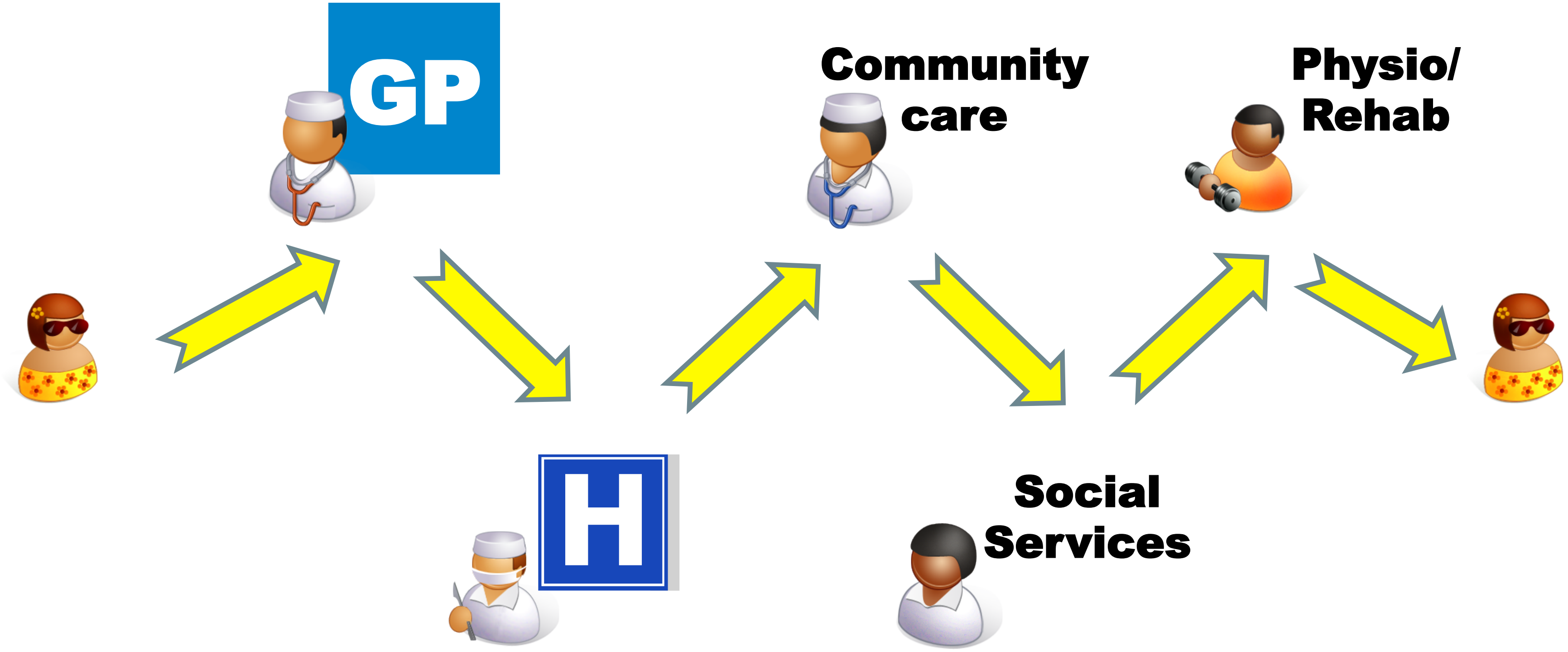
Personalised Medicine

- Personalised medicine: delivery of care tailored to the individual, their preferences and circumstances, e.g. personal health budgets
- Personalised medicines:
  - drug therapies tailored to individual patient groups to maximise effectiveness and minimise side-effects – no more ‘blockbusters’
  - Drug therapies tailored to the individual patient based on genetic markers or theranostic results – and possibly high levels of interaction/feedback to effect optimal treatment – e.g. cancer treatment ‘cocktails’

Big Data/Data-mining

- Egregiously over-hyped term …
- … but no doubt that much can be achieved in this area …
- … but may be needle-in-haystack/lottery as to whether actual results justify scale of investment …
- … but is health data different?
- need to link genomics with phenotypic and care transaction data
- how do patient outcomes vary with heredity, environment, and care delivery processes?

Typical Patient Journey



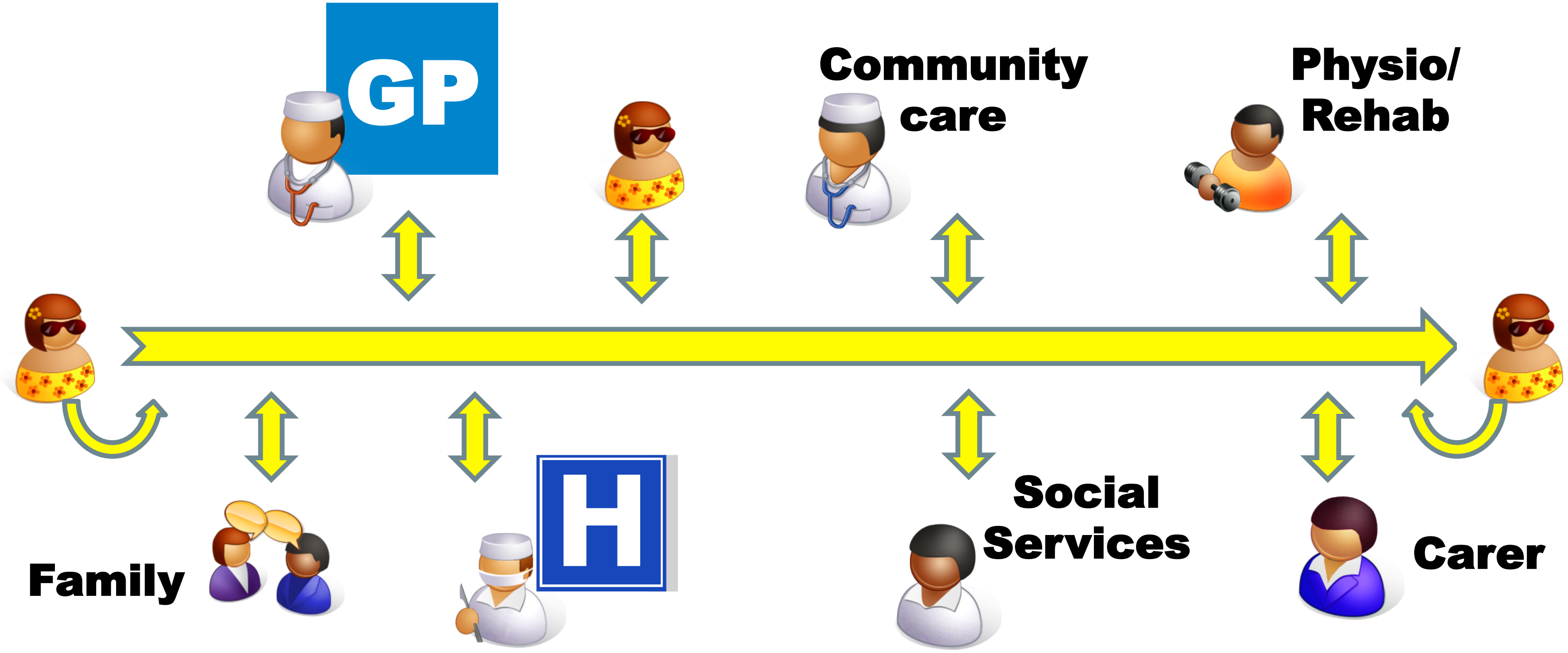
GP

Community care

Physio/ Rehab

Social Services

Coordinated Care



With a clear pathway (which allows for variations) and intelligent sharing of information to support the whole pathway.
Including the patient, carer(s)/family.

21st Century Care

- Need to support all actors in care process
- Need to support end-to-end process
- Need outcomes data – patient-reported and clinical
- Need care process data – pathways and variations – and why! Not just ‘events’ and ‘records’
- Need more on the patient’s life and lifestyle – to understand the environment and what their care preferences are or might be

So …

Need to be more intelligent about:

- care delivery
- what information is needed
- using what information we have

Need to use data more rather than less – healthcare already lags seriously behind other industries.

The 2002 Wanless report "*Securing Our Future Health: Taking A Long-Term View*" illustrated the considerable difference in expected cost depending upon how well :

- health services became more productive, and
- people became **fully engaged** with their own health.

But …

- Technical difficulties: lack of universal standards; differing incentives for ICT suppliers; lack of clear long-term strategy
- Increasing emphasis on **privacy** and individual rights rather than **confidentiality** and the common good
- Increasing caution amongst ‘gate-keepers’ about data-sharing
  - uncertainty or misinterpretation in legal position
  - ‘heads – they win; tails – I lose’ adverse incentives

EU DP Regulation

- Draft published 25th Jan 2012 by Commission
- Being reviewed in EU Parliament (LIBE) and Council of the EU (DAPIX)
- EU Parliament: over 5000 pages of amendments!
- Reconciliation Committee brings together Commission, Parliament, and Council
- Due for Dec 2013, but new Commission and Parliament in June 2014

Some Key Changes:

- ‘*Right to be forgotten*’ – unclear how far it goes
- ‘*Right to portable data*’ – good idea, but fraught with technical and logistic difficulties
- Genetic data marked out as special category of data – though no clear additional limitations
- Data about children given special status – though again not clear quite how to be treated differently
- Consent for research and statistical purposes – only (at present!) a suggested amendment
- Consent needs to be explicitly recorded – onus on data controller to prove they have consent – yet more admin!

Notable that Data Protection is now part of DG Justice rather than DG Enterprise

Implications for eHealth

- Portable data – need to determine best formats for exchanging data; need to follow standards for coding (but which ones?); need to authenticate individual and data recipient?
- Portable consent – need to manage consent along care pathways and data pathways – approaches such as miConsent and Mydex
- Protect, Inform, Provide choice, and Improve

What are we trying to protect?

- Privacy
- Confidentiality
- Security
- Data Protection

Privacy

- A right to modesty and confidential conversation
- A protection against intrusion or surveillance by state or others
- A right to control any information about oneself

First is medical courtesy, but culture-dependent;

second is ‘human right’ – ECHR Article 8;

Third is less clear-cut

We need to be sure what we mean and whether it is a ‘right’ and how to balance against other ‘rights’

Confidentiality

- A **duty** to protect interests of individual in respect of information imparted to you – presumably for a reason
- Does not forbid use of information – it is not ‘secret’ as such
- Implies some discretion in use – otherwise would be defined by contract or statute

Security

- Holding the data safe
- Permitting access to those properly authorised; preventing access by those not authorised
- Keeping complete, accurate, and available
- Business continuity planning

Data Protection

- Ensuring ‘good practice’ in terms of (commercial?) use of information – e.g. 8 ‘principles’ of the original DP Directive
- Should not include ‘human rights’ as defined elsewhere – note though Treaty of Lisbon includes ‘data protection’ as a ‘fundamental right’, though really a duty on ‘data controllers’

Risk-based approach

- Identifiable data has some risk so needs to be protected and controlled – DP Principles
- Clearly identifiable data can have ‘rights’ attached, including consent
- ‘Privacy protected’ data which is de-identified and access-controlled could be processed for broad purposes, though subject to confidentiality and non-re-identification

Implications for Healthcare

- Need to be clear about what processing is needed for good healthcare – social contract
- Need to avoid barrage of information and ‘burden’ of choice – can we provide ‘easy’ choice?
- Can we opt-out of research use of data is properly protected? The paradox of proportionality over privacy risks against public benefit in the future.
- Can we afford **not** to learn from our mistakes?