IAPP Europe Data Protection Intensive

Help or Hindrance? E-health and the Data Protection Regulation

25 April 2013

Monika McQuillen, Eversheds Switzerland,
Head of Life Sciences Group

"Europe is experiencing a strong political momentum to advance eHealth solutions for the benefit of both its citizens and health systems"

- Pēteris Zilgalvis, Head of the EC's ICT for Health Unit

Agenda

- **Introduction:** Opportunities and Risks, Context and Challenges
- **eHealth and data protection governance by hard and soft law, incl. harmonisation efforts**
    - EC White Paper: Together for Health
    - EC eHealth Action Plan 2012-2020
    - Directive 2011/24/EU: Patients' Rights in Cross-border Healthcare
    - Self-Regulatory Bodies
    - Directive 95/46/EC: Processing of Personal Data
    - National Regulator Guidance/Codes: UK example
- **New EU DP Regulation and relevance to eHealth, incl. obstacles and impact**
- **Q&A**

Introduction to eHealth
Opportunities and risks

Opportunities

- Increased sharing of healthcare data with help of technology =
  - Cost efficiency
  - Enhanced quality of healthcare services
- Mobility of healthcare, patient empowerment
- Rationalization of processes and reduced admin./medical errors
- Accessibility to data for research

Risks

- Protecting patient personal data (incl. SPD)
  - Security risks
  - Patients` rights
- Damage or damage and distress = compensation claims and enforcement action by regulator under Directive 95/46/EC
- Increased complexity of systems (interoperability)
- International competition, eg portable medical devices sector

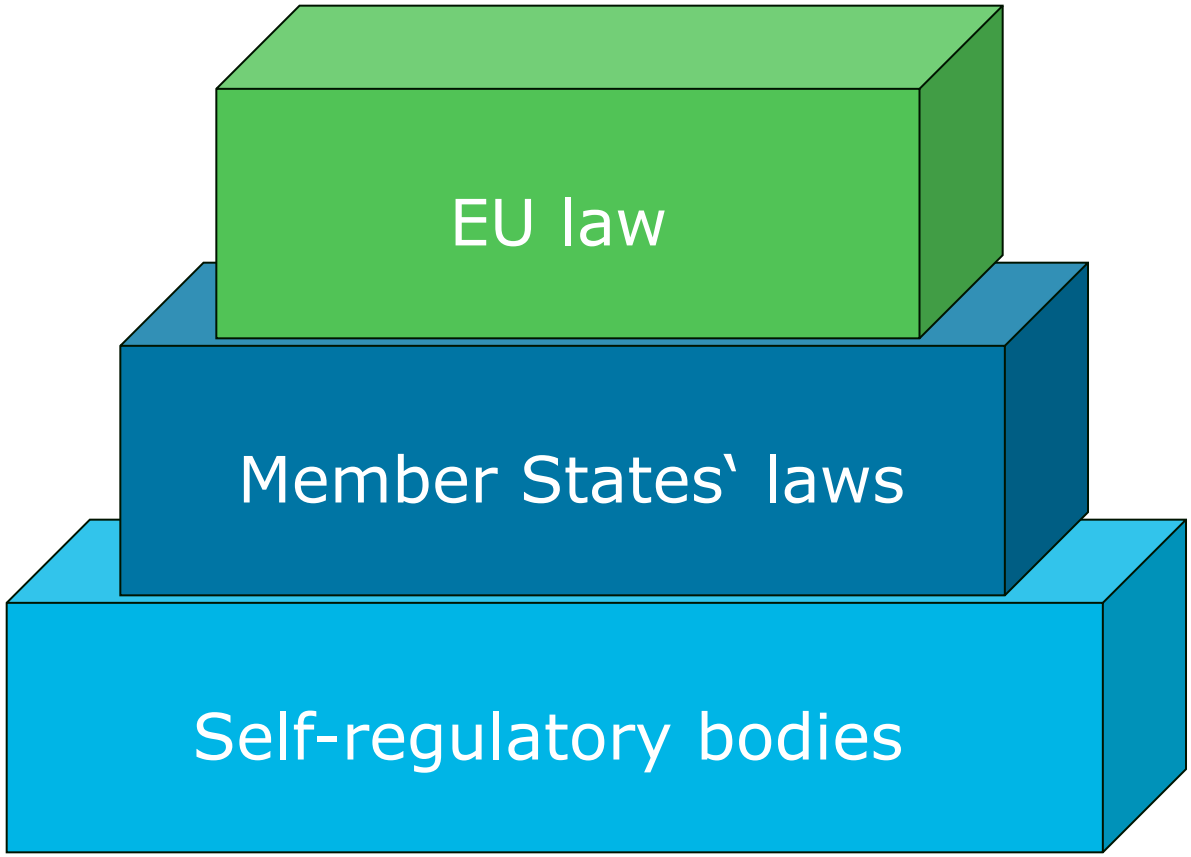
Introduction to eHealth

Context and challenges

- Data Privacy = Barrier to progress but critical to increasing patient confidence
- Strong eHealth market potential: global telemedicine market to triple to $27.3 billion by 2016
- Deployment varies between EU Member States; Denmark and Estonia success stories
- eHealth data: volume, sources, use and sharing
- Lack of EU harmonisation felt particularly in eHealth:
  - Definition of personal data itself - interpretation of "identifiable" and the approach to anonymisation
  - Scope of sensitive personal data
- EU harmonisation efforts to date…

eHealth and data protection governance

EU three tier environment; hard and soft law



Harmonisation efforts

EC Health Strategy 2008-2013

White paper "Together for Health"

Harmonisation efforts

EC eHealth Action Plan 2012-2020

- Released 7 December 2012
- Vision for future deployment of eHealth solutions; a roadmap
- Goal is threefold:
  - "Citizen-centric" healthcare
  - Increased benefits and control for patients
  - Cost efficiency
- Actions include increasing digital health literacy of EU citizens & assessing impact and value of eHealth
- Green Paper on eHealth due 2014 to address quality and transparency in eHealth market

Harmonisation efforts

Directive 2011/24/EU

- Legal framework governing a patient's right to cross-border healthcare
- Covers public and private healthcare providers
- Member States to implement by 25 October 2013
- Practical challenges: what patient data to collect and share across borders (subject always to Directive 95/46/EC and Draft EU DP Regulation)

Harmonisation efforts

Directive 2011/24/EU

- Competencies:

EU

- Rules for facilitating access to safe and high-quality cross-border healthcare
- Promote cooperation in healthcare between Member States

Member States

- Decision on types of healthcare
- Responsible for providing safe, high quality, efficient and adequate healthcare to their citizens

Harmonisation efforts

Directive 2011/24/EU: Article 14 eHealth Records

- Voluntary eHealth Network connecting national authorities responsible for eHealth
- Objectives of the eHealth Network:

Interoperable applications

European eHealth systems and services

Guidelines

List of data to be included in patient summaries which are shared across borders

Effective methods to enable use of medical information for public health and research

Support

To facilitate transferability of data in cross-border healthcare through identification and authenrication measures

Harmonisation efforts

Self-regulatory bodies

Europe

- **HON** Health on the Net Foundation, Geneva, including HON Code of Conduct

Harmonisation efforts

Directive 95/46/EC

- Member State implementation
- National variations
- Bedrock 8 principles
- New EU DP Regulation will update, but not remove, the essence of principles

Harmonisation efforts

Directive 95/46/EC

- **Principles 1 and 2** fairness and conditions for processing
- **Principle 3** adequate, relevant, not excessive for purpose
- **Principle 4** accurate and up to date
- **Principle 5** data retention
- **Principle 6** Data Subject rights incl. access/copies, compensation for damage or damage and distress, rectification, blocking, erasure and destruction
- **Principle 7** data security
- **Principle 8** data transfers outside EEA

New EU DP Regulation: All change?
What and when?

- Draft published by EU Commission on 25 January 2012
- Replace Directive 95/46/EC and increase harmonisation
- Likely 2 years for legislative process to complete; further 2 years to come into **direct** effect; Member States to repeal current enactment of Directive 95/46/EC
- Stakeholder groups are entitled to comment

New EU DP Regulation: All change?

Overview

- Movement towards more prescriptive rules (for harmonisation)
  - Helpful re commonality of definitions
  - Retention of many current concepts, definitions, principles including sensitive data distinction
  - Broader and deeper compliance obligations which will impact eHealth

New EU DP Regulation: All change?

Overview

- *"…one, single,* ***technologically neutral and future-proof set of rules across the EU…Regardless of how technology…develops in the future****, the personal information of individuals in the EU will be secure, and their fundamental right to data protection respected."*

  EU Commission Fact Sheet: "How reform will adapt data protection rules to new technological developments"

New EU DP Regulation: All change?

Territorial scope (Article 3)

- Expanded to Data Controller not established in EU

Example: US company who provides a web portal that provides services to EU residents and monitors the use of the portal and data collected on the portal now falls under the proposed regulation

- To protect EU residents beyond their borders

Implications for eHealth?

- Increased reach of patient protections

New EU DP Regulation: All change?

Mandatory data security breach reporting (Article 31)

- Data Controller **must** notify and provide details to supervisory authority of **all** Personal Data breaches (not just serious) without delay and, where feasible, within 24 hours after becoming aware
- Data Processor must alert Data Controller **immediately**

Implications for eHealth?

- Facilitating transparency, patient control and remedial action to contain and mitigate risk
- Service provider direct obligation under EU law to alert Data Controller

New EU DP Regulation: All change?

Mandatory data privacy impact assessments (Article 33)

- Data Controllers and Data Processors must undertake DPIA before "risky" processing operations
- DPIA indicating high risk = consultation obligation with supervisory authority

Implications for eHealth?

- Particular application and frequency of DPIAs
- Draft mentions specific operations eg:
  - systematic and extensive evaluation for analysing or predicting a person's **health**
  - processing of **SPD**
  - and systems on **genetics or biometric data**

New EU DP Regulation: All change?

Increased sanctions for non-compliance including a three-tier system (Article 79)

- Fines of up to 2% annual worldwide turnover
- Sanctions not necessarily based on actual harm to individual eg patient

Implications for eHealth?

- Even more reason to protect patient data
- First time for fines as percentage of turnover
- Likely application of uppermost tier to eHealth data which is not anonymised
- NB: Possible fines **even if** no harm to patient

New EU DP Regulation: All change?

Positive consent obligations (Article 7)

- Consent must be "explicit"; plus further conditions
- Controller burden of proof
- Data Subject's right to withdraw consent at any time
- Consent no legal basis for processing where significant imbalance between Data Subject and Data Controller

Implications for eHealth?

- Explicit consent for SPD processing is not new
- Neither is risk of withdrawal or question about validity if unequal bargaining power
- Additional limitations around consent are new, hence increased need for reliance on alternatives

New EU DP Regulation: All change?

The Right to be Forgotten

- 'Right to be forgotten': if no legitimate reason for an organisation to keep data, it must be removed from their system at request of Data Subject
- One of the following grounds must apply:
  - Data no longer necessary in relation to the purpose for which they were collected
  - The data subject withdraws consent or the storage period has expired and no other legal ground remains
  - The data subject objects to the processing under Art. 19
  - Processing does not comply with the regulation

New EU DP Regulation: All change?

Enhanced Data Subject control (Articles 12, 17, 18)

- Broader objection rights, eg:
  - right of access including right to increased information from Data Controller
  - right to rectification
  - right to erasure without delay
  - right to abstain from onward dissemination
- 'Data portability': right to obtain copy from one entity and transmit it to another without hindrance

Implications for eHealth?

- Patient trust and confidence

New EU DP Regulation: All change?

International transfers (Articles 41, 43 and 44)

- The proposals build on the existing mechanisms and provide a detailed framework for transfers of Personal Data outside EEA

Implications for eHealth?

- Providers of eHealth products/services and who process data outside EEA will be seeking more practical data transfer rules
- Current regime inadequate; heavy reliance on impractical EU Model Clauses and Safe Harbor; limitations of both
- Caution: Draft inadequate to address practical difficulties

New EU DP Regulation: All change?

Data Processor obligations (Articles 4, 28 and 30)

- Express obligations on Data Processors is significant change from Directive 95/46/EC
- eg to cooperate with supervisory authorities, keep secure and keep records of processing operations

Implications for eHealth?

- Previous risk: breach of contract to Data Controller
- Providers of eHealth related products and services to their Data Controller customers will for the first time be caught by direct obligations, including eg security

New EU DP Regulation: All change?

Privacy by Design and by Default (Article 23)

- Data Privacy embedded throughout eg product life cycle
- Data Controllers must consider appropriate technical and organisational security measures when deciding means for processing and at time of processing
- Default: Data Controllers must only collect, process and retain Personal Data necessary for purpose and must ensure "need to know" strictly necessary access only
- Qualification: *"Having regard to the state of the art and the cost of implementation…"*

New EU DP Regulation: All change?

Obstacles facing eHealth (Articles 81, 83)

- Personal data concerning health must be processed within legal safeguards that protect legitimate interests and be necessary for:
  - preventive or occupational medicine, medical diagnosis, providing care/treatment or management of health-care services
  - reasons of public interest in the area of public health; or
  - other reasons of public interest eg ensuring cost effective settling of claims in health insurance system

- Restrictions on processing for historical, statistical or scientific research purposes

New EU DP Regulation: All change?

Impact on pharma industry (Article 83)

- **Need to protect research**
  - Wellcome Trust (Response to Justice Select Committee: Inquiry on EU Data Protection Framework Proposals)
  - FEAM (Federation of European Academies of Medicine)

New EU DP Regulation: All change?

Preparing for impact

- Plans for new eHealth initiatives/products/processing?

  Factor in DPIA (Data Controller and Data Processor) and Privacy By Design (Data Controller only).
- Established outside EU but processing EU patient data?

  Keep in mind new territoriality extension.
- Data Processor role?

  Keep in mind new direct obligations.
- Will new patient rights be protected?

  Keep in mind new 'Right to be forgotten', data portability, rights of access and rectification.
- Actual or suspected, threatened or "near miss" security breach?

  Keep in mind new mandatory breach notification and risk of uppermost tier of fine. Check your internal security measures and those of subcontractors/agents.

Resource links

White Paper: Together for Health
http://ec.europa.eu/health/ph_overview/Documents/strategy_wp_en.pdf
Directive 2011/24/EU: Patients' Rights in Cross-border Healthcare & European Patients' Forum
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:088:0045:0065:EN:PDF
http://www.eu-patient.eu/Documents/Policy/Cross-borderHealthcare/EPF%20Guidance%20on%20Cross-Border%20Healthcare.pdf
eHealth Action Plan 2012-2020 & European Public Health Alliance
https://ec.europa.eu/digital-agenda/en/news/ehealth-action-plan-2012-2020-innovative-healthcare-21st-century
http://www.epha.org/a/5490
http://europa.eu/rapid/press-release_MEMO-12-959_en.htm
Health on the Net Foundation, Geneva
http://www.hon.ch/
UK ICO Guidance and Codes
http://www.ico.gov.uk/
http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/anonymisation.aspx
http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/data_sharing.aspx
http://www.ico.gov.uk/~/media/documents/library/Data_Protection/Practical_application/BREACH_REPORTING.ashx
http://www.ico.gov.uk/news/current_topics/Our_approach_to_encryption.aspx
DP Regulation draft of 25 January 2012 and EU Fact Sheet
http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf
http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/8_en.pdf
http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm
Wellcome Trust (Response to Justice Select Committee: Inquiry on EU Data Protection Framework Proposals) August 2012
http://www.wellcome.ac.uk/stellent/groups/corporatesite/@policy_communications/documents/web_document/wtp040618.pdf
FEAM (Federation of European Academies of Medicine)
http://www.feam-site.eu/cms/docs/publications/FEAMDataProtectionStatementJune2012.pdf

Q&A session

- Monika McQuillen: +41 44 20 49 09 7
  (monika.mcquillen@eversheds.ch)
- Eversheds Ltd.
  Stadelhoferstrasse 22
  8001 Zurich