Data Protection and Innovation
Can we strike a balance?

Zoi Kolitsi
Informatics and Information Security Laboratory
Aristotelian University of Thessaloniki, Greece
Health care is special...

- Health systems linked to culture and social policies
- In Europe, subsidiarity principle
  - Co-operation on public health matters BUT
  - No harmonization of MS health care legislation
  - Member States have full control on how they organize their systems

**H owever**

- Substantial variations between national health care systems, but also similar challenges are faced and
- substantial similarities in political ambitions to reform health care as well as in the challenges to reach these goals
Health Data is special...

Data from SPECIAL EUROBAROMETER 359 Report, *Attitudes on Data Protection and Electronic Identity in the European Union*, June 2011

HL7 International 28th Annual Plenary & Working Group Meeting, Chicago, 14-19 Sept, 2014
Health Data requires a high level of protection...

- Data Protection a critical matter for data processing in eHealth
  - Legal basis for data processing is necessary
  - Ethical, regulatory and human rights instruments are also relevant.

- Large Diversity across countries
  - Challenging when crossing national and professional boundaries

Need to strike a balance between achieving a consistent level of data protection and rights, removing obstacles and cutting red tape.
Different purpose, different needs...

For care purposes
- information sharing within the same context is done on a “need to share” basis within a defined healthcare team.
Health and medical institutions are trusted ...

Data from SPECIAL EUROBAROMETER 359 Report, *Attitudes on Data Protection and Electronic Identity in the European Union*, June 2011
Beyond team based health care

- wide variety of potential “secondary” use of data open to healthcare professionals outside the team, social care providers, insurers, technical staff, researchers, and others
- Data re-use made possible in other sectors but major challenges remain in eHealth
  - * * * Semantic Interoperability and legal barriers
Mobile applications in health

- Extramural care and remote monitoring, patients on the move
- Extensive use of smart phones and proliferation of apps
- User identifiable data on location and access to info on the web
Big Data Analytics

• Potential to create new knowledge in research and enormous benefits for governments to improve health service delivery and detect fraud.
• A market eager to exploit business use cases leveraging such potential
• No real controls and limited citizen knowledge of the risks or informed consent
• Need for policies and laws to protect privacy

- Big data tools can alter the balance of power between government and citizen.
- Big data tools can reveal intimate personal details.
- Big data tools could lead to discriminatory outcomes.

Big Data: Seizing Opportunities, preserving values, Executive Office of the President, May 2014
Key messages from international collaboration

- **epSOS** - a Large Scale Pilot for data sharing across borders in Europe
  - **Trillium Bridge** investigating the transatlantic dimension
- **CALLIOPE** – a Thematic Network for eHealth interoperability, delivered the eHealth Interoperability Roadmap
- **eHGI** – eHealth Governance Initiative supporting the policy co-ordination process
- **eSENS** – a Large scale pilot for cross sectoral interoperability
Working together to tackle common challenges

• Policy level: the Article 14* eHealth Network
  ▫ members are high level policy officials of national health administrations
• Strategy Level: Support mechanisms and Joint actions to consolidate national experience and recommendations from pilots
• Implementation level: Common large scale pilots, Networks, Stakeholder engagement

*of Directive 2011/24
Address simultaneously all levels of interoperability in a step by step approach

CALLIOPE Interoperability Road map, December 2010

HL7 International 28th Annual Plenary &Working Group Meeting, Chicago, 14-19 Sept, 2014
Critical Issues for eHealth

- Establishing maintaining and safeguarding trust in the EU/international context
- Authorizations to access data, including patient consent
- Specific identification challenges
- Privacy by design
- Accountability, traceability and audit
- Creating and maintaining convergence
- Patient Access to own health data - opportunities and limitations
Legal Interoperability Agreements

The epSOS Approach*

- In compliance with EU and National Legislation
- Addressing diversity

- Pre-requisite: a solid governance framework

*NOTE: Positively considered by the DPAs (WP29 working document on epSOS)

Adopted EU level epSOS Iop Agreement

Localisation of the Agreement

Implementation of the Agreement

Self-assessment and Audit against the Agreement

Reporting on results of self-assessment

Entry into the pilot

Monitoring and audit
From Interoperability Agreements to Legal Action

- Recommendations form pilots
- Policy development
- Adoption of guidelines
- Voluntary national action for cross border interoperability
Tackle horizontal legal issues for a stepwise approach

**Horizontal issues**

- establishing and safeguarding trust
- Common policies, measures (e.g. NCPeH, circle of trust, eID for eHealth, secondary use of data)
- Co-ordination and Collaborative Governance (agreements, monitoring, arbitration)

**Use case specific issues**

- Seamless security and trust across all players of the value chain
- Use case specific regulations (risk adjusted access policies, medicines, reimbursement, clinical trials...)
- Organizational, viability and sustainability aspects
... and yes, eHealth is special!

- Cross sectoral eID and use of eSignatures in eHealth may be considered (identification and authentication) but authorization is a complex eHealth issue
- Semantic interoperability aspects are far more complex and involved
- Engagement of stakeholders –especially end users and industry is a must
- A good level of collaborative governance is a pre-requisite
LEGISLATION
Modernization of Data Protection Legislation

IN EUROPE

• Data Protection
  ▫ A (General) a EU Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data
  ▫ To be applied and enforced **nationally**
  ▫ In process of approval, to succeed the Data Protection Directive

• Electronic identification and trust services
  ▫ EU Regulation on electronic identification and trust services for electronic transactions in the internal market, published July 2014

• Standardization
  ▫ the European Standardization Regulation which impacts primarily on the adoption of technical specifications in the domain of ICT, October 2012

- Advance the Consumer Privacy Bill of Rights.
- Pass national data breach legislation.
- ...........
- Amend the Electronic Communications Privacy Act.

Big Data: Seizing Opportunities, preserving values, Executive Office of the President, May 2014
Three main Innovations in the EU Data Protection Reform (in process)

- **One continent, one law**: single, pan-European law for data protection, Companies will deal with one law, not 28.

- **One-stop-shop** for businesses: companies will only have to deal with one single supervisory authority

- **The same rules for all companies – regardless of their establishment**: companies based outside of Europe will have to apply the same rules. Companies with strong procedures for protecting personal data will have a competitive advantage on a global scale at a time when the issue is becoming increasingly sensitive.

The benefits are estimated at €2.3 billion per year.

- **Extend privacy protections to non-US persons.**

Big Data: Seizing Opportunities, preserving values, Executive Office of the President, May 2014
Highlights

• Protection of personal data balanced with other fundamental rights, in accordance with the principle of proportionality.
• Protection of individuals should be technologically neutral
• Clarity on “person identifiable data”
• Citizens in control — provisions for information and freely-given, specific and informed consent, provided unambiguously by any appropriate method
• Genetic data is personal data
• Impact analysis
• Ensuring appropriate security levels
• The right to be forgotten — adjusted to societal needs
• Data Portability
• Health specific provisions!
Specifically for Big Data Analytics

- **Accountability** and social responsibility a global competitive advantage - Impact Analysis and risk adjusted security.
- Promotes honest communication and unambiguous information on the impacts to personal privacy from big data and analytics in each and every situation.
- Emergence of the informed consumer that can weigh the benefits and the risks.
- The state provides control, enforcement and redress mechanisms.
- Strict and austere consequences for breaches.
Specifically for eHealth (in discussion)

- Processing of personal data for health-related purposes
- Processing for purposes of social protection*
- Processing of personal data for archiving purposes in the public interest *
- Processing of personal data for statistical and scientific purposes*

* Member State law / the controller shall provide for specific and suitable measures to safeguard the rights and freedoms of the data subject...
GOVERNANCE
The case of re-using identifiable health data

• Providing specific, informed prior consent is not possible and per case consent has a huge organizational overhead
• Re-using data without citizens being informed is out of consideration
  ➢ MS deciding for their own? Obstacles to research relying on international evidence.
  ➢ A common policy on controllers responsibilities?
    ▪ Common principles, need for safeguards and measures
    ▪ National level derogations (for reducing burden)
In addition to legislation

- **Layered Governance - International (Union), national, organization**
- **Collaborative**
  - Together with competence centers, stakeholders and experts
  - Define measures and safeguards
  - Propose methods and solutions
- **Co-ordination**
  - at the political/policy level (in Europe the eHealth Network)
  - Adopt guidelines
  - Voluntarily evolve national regulatory framework

- Trusted eHealth National Contact Points
- Patient access to Electronic Health Records and health data portability
- Electronic Identification for eHealth
- Secondary use of Medical Data
- Implementation of legal interoperability (Guidelines)
- Implementation of data protection Regulation in eHealth
Thank you!

e-mail: kolitsi@vivodinet.gr