THE EHR PRIVACY APPROACH AND LEGAL ISSUES AROUND THE RE-USE OF DATA

Dr. Petra Wilson, IDF
Prof. Nikolaus Forgo, CDP
Peter Singleton, UCL
Addressing key questions around privacy

- **Petra Wilson** – Chief Executive at International Diabetes Federation and Member of the EHR4CR Ethics Board
- **Nikolaus Forgo** – President at Centre for Data Protection and Director of the Institute for Legal Informatics at the University of Hannover
- **Peter Singleton** – Senior Research Fellow, Centre for Health Informatics and Multi-professional Education (CHIME) at UCL
PRIVACY PROTECTION FROM AN INTERNATIONAL PERSPECTIVE

Dr. Petra Wilson
International Diabetes Federation
Legal Constructions of Privacy

Global eHealth Observatory Report
Global eHealth Resolution

- The World Health Organization's eHealth resolution WHA 58.28 (2005) seeks to:
  - strengthen health systems through the use of eHealth;
  - build public-private partnerships in ICT development and deployment for health;
  - support capacity building for the application of eHealth;
  - support development and adoption of standards;
  - monitoring, documenting and analysing trends and developments in eHealth and publishing the results to promote better understanding.
- Second survey in six reports published during 2010 and 2012
- Legal frameworks for eHealth - 1 February 2012
Global eHealth Survey 2009 – response rate

<table>
<thead>
<tr>
<th>WHO Region</th>
<th>Africa</th>
<th>Americas</th>
<th>S-East Asia</th>
<th>Europe</th>
<th>Eastern Mediterr.</th>
<th>Western Pacific</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total countries</td>
<td>46</td>
<td>35</td>
<td>11</td>
<td>53</td>
<td>21</td>
<td>27</td>
</tr>
<tr>
<td>responding countries</td>
<td>30</td>
<td>12</td>
<td>8</td>
<td>36</td>
<td>14</td>
<td>13</td>
</tr>
<tr>
<td>Response rate</td>
<td>65%</td>
<td>34%</td>
<td>73%</td>
<td>68%</td>
<td>67%</td>
<td>48%</td>
</tr>
</tbody>
</table>
Global eHealth Survey 2009 – the legal questions

- Does your country have legislation to ensure privacy of personally identifiable data of individuals irrespective of whether it is in analog or digital format?
- Does your country have specific legislation to protect privacy of individuals' health-related data held in digitized format in an EMR or EHR?
- Does your country have legislation which provides for the sharing of health-related data between health care staff through an EHR?
- Does your country have legislation which grants the right of access by individuals of their health-related data when held in an EHR?
- Does your country have legislation which allows for the transmission and sharing of research data containing personal and health-related data between research entities in different countries?
Does your country have legislation to ensure privacy of personally identifiable data of individuals irrespective of whether it is in analog or digital format?
Does your country have specific legislation to protect privacy of individuals' health-related data held in digitized format in an EMR or EHR?
Use of Electronic Format for Health Records

Local health care facilities:
Individual patient information

Percent of countries

Paper
Electronic
Transmission

Very high
High
Medium
Low
None
No answer

Electronic Health Records for Clinical Research
Does your country have legislation which provides for the sharing of health-related data between health care staff through an EHR within the same health care entity?
Does your country have legislation which provides for the sharing of health-related data with health care entities in other countries?
Does your country have legislation which grants the right of access by individuals of their health-related data when held in an EHR?
Does your country have legislation which allows for the transmission and sharing of research data containing personal and health-related data between research entities in different countries?
General Conclusions - Basics in place

- Generally good levels of basic rights to information privacy exist globally.
- Specific health information privacy protection is not as widely present and is often contained in professional codes of conduct rather than law.
- Legislation specifically aimed at protecting privacy in EHRs is limited to countries where considerable deployment of EHRs already exists.
- Laws and regulation on the use of EHRs tend to be reactive - few States use legislation as a tool to facilitate and drive uptake of EHRs
- Legislation tends to be restrictive rather than facilitative
General Conclusions - Building Trust

- Adaptations should be made to existing legal frameworks to ensure that data can be shared appropriately to provide patient care and support wider public health initiatives.

- This requires:
  - Building patient trust should by giving patients more information about how their data are handled and providing education on the technical and regulatory requirements of privacy and security which are used to ensure that data are shared appropriately.
  - Driving healthcare professional engagement in using EHR data for better healthcare delivery.
  - Educating all stakeholders on potential for EHR use for direct care and care planning
General Conclusions – next steps

- Legislation should be adopted to ensure that patient data can be shared safely for **direct patient care**.

- Legislation should be adopted to facilitate appropriate use of EHRs for **research**.

- Patients should be empowered to make their data available for secondary research through easily understandable and applicable privacy legislation.

- New legislative approaches should be adopted to support a suitable **balance** between accessibility of data and the levels of privacy patients wish to maintain.
The big shift?

- Changing the legal constructions of electronic health data
  - from ownership to control
  - from a reference resource to a key healthcare asset
  - from an individual good to a national resource

Petra.wilson@idf.org
LEGAL ISSUES IN CONNECTION WITH THE RE-USE OF EHR DATA

Prof. Nikolaus Forgo
Centre for Data Protection
Leibniz Universität Hannover
Lessons learnt on data re-use in Europe
My Background
Golden Rule

Processing of personal data is only allowed if:

• it is permitted by law or

• the data subject has consented to it
Hitting the balance

All kinds of troubles …
Outcomes

Stu’s Views © 2002 Stu All Rights Reserved www.stus.com

Attorneys rarely survive in the wild

“But I came here to negotiate.”
2 Main approaches

- Aggregation/K-Anonymity/Noise
- De-facto Anonymity
Advantages: Aggregation

- No central entity
- No legal paperwork
- Responsibility remains with the data providers

Advantages: De-facto-Anonymity

- Central Entity
- Legal roles clearly defined
- Responsibility is (in parts) shifted to a central entity
- Reidentification possible
Disadvantages: Aggregation

- Anonymity questionable
- Anonymity at risk
- Legal status untested
- Responsibility unclear
- Legal rules unexistent
- Reidentification impossible

Disadvantages: De-facto-Anonymity

- Sustainability of central entity unclear
- Signing process costly and time consuming
- Concept complex and (local) ethics committees and DPAs need to understand it
- Scalability → Participation needs signing
Since January 2012

COM(2012) 11 final
2012/0011 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)
A fine, up to **100 000 000 EUR**, or up to 5% of the annual worldwide turnover in case of an enterprise, whichever is greater.
Thank you!

This project has received funding from the European Union’s Seventh Framework Programme for research, technological development and demonstration under grant agreement no 270089.
Contact Details

Nikolaus Forgó
Institute for Legal Informatics
Leibniz Universität Hannover
Juristische Fakultät
Königsworther Platz 1
D-30167 Hannover

Tel: + 49 511 762 8159
Fax: + 49 511 762 8290
E-Mail: nikolaus.forgo@iri.uni-hannover.de
Web: http://www.iri.uni-hannover.de
Twitter: @nikolausf
THE EHR4CR PRIVACY APPROACH

Peter Singleton
University College London
EHR4CR Overview – data flow

**RESEARCH CENTRE**
e.g. pharmaceutical company

**EHR4CR PLATFORM**

**HOSPITAL/DATA PROVIDER**

1. **FEASIBILITY**

   - QUERY WORKBENCH
   - STUDY CRITERIA
   - QUERY
   - #COUNT
   - RECRUITMENT PROGRESS
   - EHR4CR SERVICES

2. **RECRUITMENT**

   - QUERY WORKBENCH
   - CLINICAL DATA WAREHOUSE
   - QUERY
   - CANDIDATE LIST
   - ELECTRONIC CASE REPORT FORM

3. **EHR**

   - EXTRACT, TRANSFORM, LOAD

   QUERIES AND RESULTS ACROSS MULTIPLE SITES

**ELECTRONIC HEALTH RECORDS FOR CLINICAL RESEARCH**

**BRUSSELS - 9 APRIL 2014**

177
The EHR4CR privacy and legal framework was built upon experience and broad consultation

- Previous EU projects informed the policy development:
  - ACGT – Supporting clinical trials in cancer
  - DebugIT – sharing infection and response data
  - VPH-Share – open framework for bioscience

- EHR4CR Consultations

- Convergence Initiative – working with other EU projects: p-Medicine, PONTE, CONTRACT, EPSOS
Privacy protection delivered on multiple levels

- Personal data only processed by original data controller (treating physician)
  - EHR4CR only handles aggregate data with additional protections
- Clinical Data Warehouse holds only pseudonymous data
- Role-based access controls to limit access to aggregate data
- Extensive audit trails with reporting
- Integration of Operating Procedures with system functionality
Governance tools are vital to safeguard data

Ensures consistent application of principles and legal requirements and to aid adoption of best practice

- Standard Operating Rules
- Standard Operating Procedure outline templates
- Contract and Agreement templates or Heads of Agreement
- Standard training materials
Standard Operating Rules

- General
- Context-dependent
  - Specific for each scenario
- Access Controls
- Audit & Monitoring
- Non-Compliance
- Risk Management
- Incident Management and Reporting