Liability, Privacy and Security in Medical Data Sharing: the Swiss Experience

Ria Kechagia
Juan Ramón Troncoso-Pastoriza

ria.kechagia@epfl.ch
juan.troncoso-pastoriza@epfl.ch

Outline

- Introduction
  - Facts about medical research data
  - Data Protection in Personalized Health Project
- Liability
  - Legal framework
  - Challenges
  - Conclusions
- Privacy and Security Threats to Personalized Medicine
  - Security and Privacy Technologies
  - MedCo: Privacy-Conscious Exploration of Distributed Clinical and Genomic Data
  - Related Events and Publications
- Conclusions and Open Questions

Growing Concern: Medical Data Breaches

Around 5 declared breaches per week, each affecting 500+ people

https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

Welcome | File a Breach | HHS | Office for Civil Rights | Contact Us

U.S. Department of Health and Human Services
Office for Civil Rights
Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information

Under Investigation | Archive | Help for Consumers

As required by section 13402(e)(4) of the HITECH Act, the Secretary must post a list of breaches of unsecured protected health information affecting 500 or more individuals. The following breaches have been reported to the Secretary:

Cases Currently Under Investigation

This page lists all breaches reported within the last 24 months that are currently under investigation by the Office for Civil Rights.

Show Advanced Options

Breach Report Results

Expand All	Name of Covered Entity	State	Covered Entity Type	Individuals Affected	Breach Submission Date	Type of Breach	Location of Breached Information
	Kansas City VAMC	MO	Healthcare Provider	534	06/11/2019	Unauthorized Access/Disclosure	Paper/Films
	Worcester Eye Consultants	MA	Healthcare Provider	2634	06/07/2019	Loss	Other
	Rosenbaum Dental Group	FL	Healthcare Provider	1200	06/04/2019	Hacking/IT Incident	Desktop Computer
	Humana Inc	KY	Health Plan	863	06/03/2019	Unauthorized Access/Disclosure	Network Server
	Broome County, New York	NY	Healthcare Provider	7048	05/31/2019	Hacking/IT Incident	Email
	The Union Labor Life Insurance Company	MD	Health Plan	87400	05/31/2019	Hacking/IT Incident	Email

Recent targeted Attacks (2016-2018)

Do state institutions have the resources to fight hackers?

Public sector has lessons to learn as hospital trusts and GPs struggle to recover from ransomware attack

20. März 2016, 10:05 Uhr Klinikum Neuss

Wenn Cyberkriminelle ein Krankenhaus lahmlegen

Das Lukaskrankenhaus der Städtischen Kliniken in Neuss wurde Opfer von Cyberkriminellen. (Foto: dpa)

The Telegraph HOME | NEWS | SP

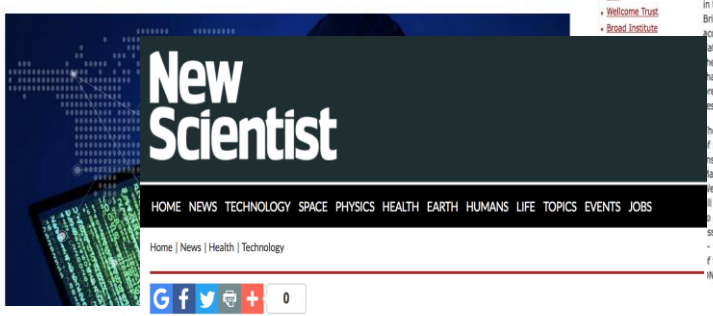
News

UK | World | Politics | Science | Education | Health | Brexit | Royals | Investigat

News

NHS patients' genetic data targeted as foreign hackers attack high security MoD unit

share Save 33



DAILY NEWS 1 September 2008

Genetic data withdrawn amid privacy concerns

By Peter Aldhous

nature International weekly journal of science

Subscribe Login

nature news home | news archive | specials | opinion | features | news blog | nature journal

comments on this story

Stories by subject
- Genetics
- Health and medicine
- Policy

Stories by keywords
- NIH
- Wellcome Trust
- Broad Institute

Published online 4 September 2008 | Nature | doi:10.1038/news.2008.1083

News

Researchers criticize genetic data restrictions

Fears over privacy breaches are premature and will impede research, experts say.

Natasha Gilbert

As fears over privacy prompt genetic databases in the United States and Britain to close public access to some of their data, scientists working in the field are complaining that the moves are premature and will impede research.

The US National Institutes of Health (NIH), the Broad Institute in Cambridge, Massachusetts, and the Wellcome Trust in London have all decided to restrict access to data from genome-wide association (GWA) studies – which contain collections of thousands of people's DNA – after research

Could an individual's health details be extracted from pooled genetic data?

Getty

Related stories
- Biomedical science: Betting the bank 23 April 2008
- Genome studies: Genetics by numbers 30 January 2008

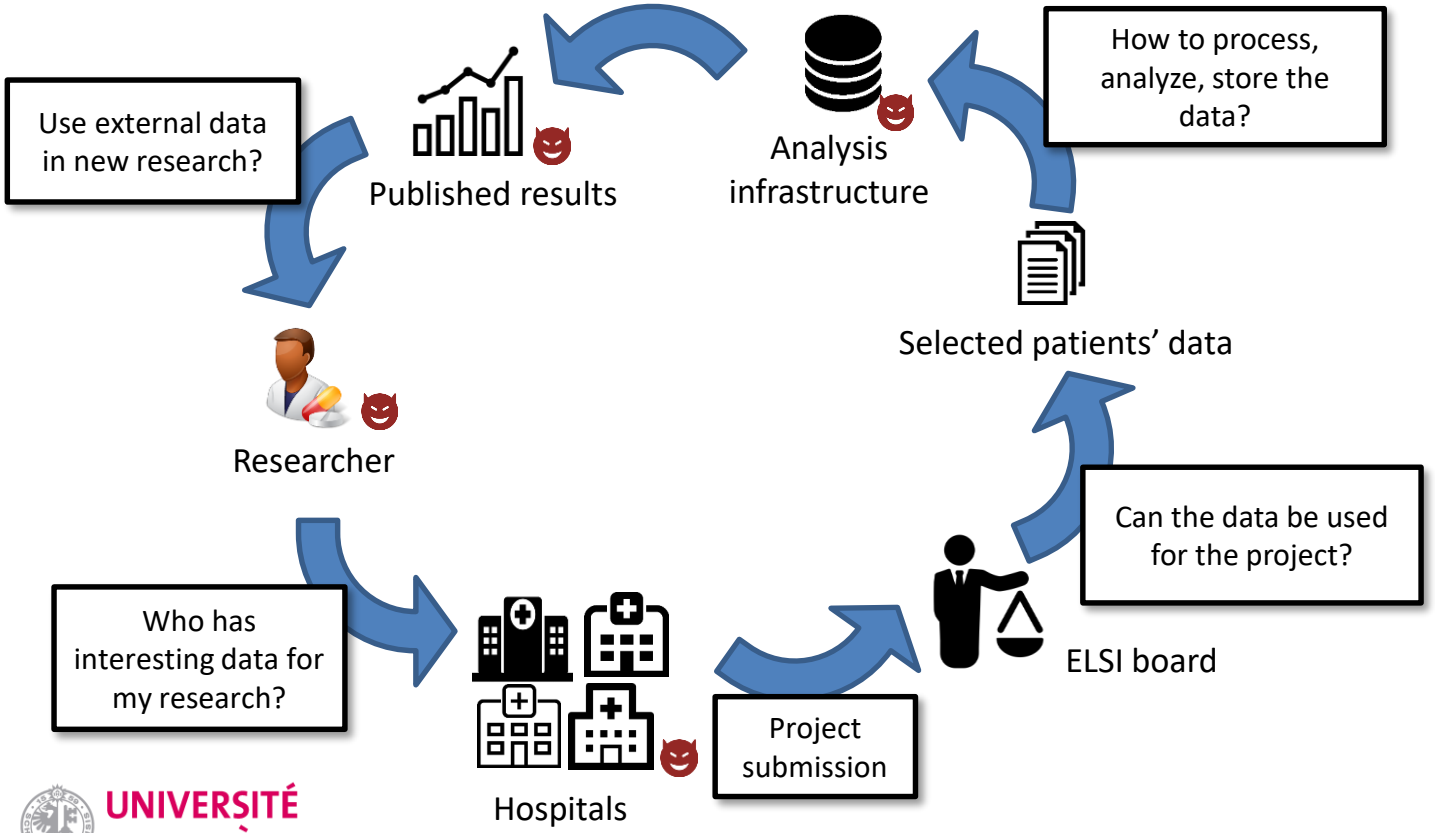
Naturejobs
- Gastroenterologist Loyola University Chicago
- Research Engineer / Research Scientist in Renewable Energy King Fahd University of Petroleum & Minerals
- More science jobs
- Post a job

Resources
- Send to a Friend
- Reprints & Permissions
- RSS Feeds

elsewhere on nature.com
- Genetics@nature.com

UNIVERSITÉ DE GENÈVE EPFL

Clinical Research Process



Clinical Data

- Structured EHR (LDEP, 2009)
- Unstructured EHR
- Medical Images

Genomic Data

- DNA sequences

Behavior Data

- Social networks
- Wearables

Liability notions

Liability and Medical Research Data in Switzerland: The legal framework

- Human Research Act (HRA)
- Data Protection Legislation (Federal Act on Data Protection (FADP), Ordinance

concerning the federal law on the protection of data (OLPD)

- Swiss Civil Code on the Protection of Personality Art.28-28l
- Health Insurance Act
- Therapeutic Products Act
- General tort law (Art. 41) and Product Liability Act 1994
- Federal Constitution Art. 13 on the Protection of Privacy
- GDPR

Liability and Medical Research Data in Switzerland: Scope and Conditions of HRA

HRA applies to research concerning human diseases and concerning the structure and function of the human body which involves a person's biological material and health-related personal data

Art. 19 Liability 1 Any person who carries out a research project involving persons shall be liable for damage suffered by them in connection with the project.

However, HRA does not apply to anonymized biological material and anonymously collected or anonymized health-related data.

Liability and Medical Research Data in Switzerland: Data Protection Legislation

Federal Data Protection Act: Art. 13 Justification in processing personal data by private persons:
"[1] A breach of privacy is unlawful unless it is justified by the consent of the injured party, by an overriding private or public interest or by law.
[2] An overriding interest of the person processing the data shall in particular be considered if that person:
[…] e. processes personal data for purposes not relating to a specific person, in particular *for the purposes of research* […] and *publishes* the results in such a manner that the *data subjects may not be identified*".

Ordinance: Art. 8 General measures 1
Anyone who as private individual processes personal data or provides a data communication network shall ensure the confidentiality, availability and the integrity of the data in order to ensure an appropriate level of data protection.
In particular, he shall protect the systems against the following risks:
a. unauthorised or accidental destruction;
b. accidental loss;
c. c. technical faults;
d. forgery, theft or unlawful use;
e. unauthorised alteration, copying, access or other unauthorised processing.

Legal Challenges Regarding Medical Research Data (incl. Genomic)

In general:

- Informed Consent
- Ownership of data
- Codes of conduct for the researchers
- Management of sensitive Big Data (storage and accessibility)
- Genomic data not fully anonymizable

Liability connected:

- New DPA
- 26 different legislations per canton
- Adaptation to the parallel developments in Switzerland: SPHN
- Disclosure of secondary finding to patients: Researcher liable?
- GDPR compatibility: Liability vs. Accountability (Art. 5 GDPR, Recital 74)

Conclusions:

- The applicable law on assessing liability for the breaches of medical data depends on the type of research and the data involved.

- There are many ethical, legal and technological challenges regarding the regulation of the use medical research data in the context of Precision Medicine that need to be addressed.

Security and Privacy in Personalized Medicine

Technologies for Privacy Protection

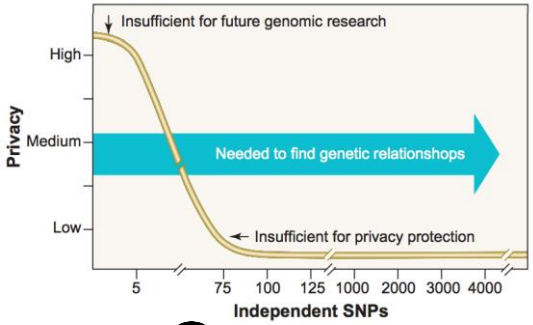
A Plethora of Attacks Against Genomic Privacy

Lin et al. 2004 Science: 75 or more SNPs (Single Nucleotide Polymorphisms) are sufficient to identify a single person

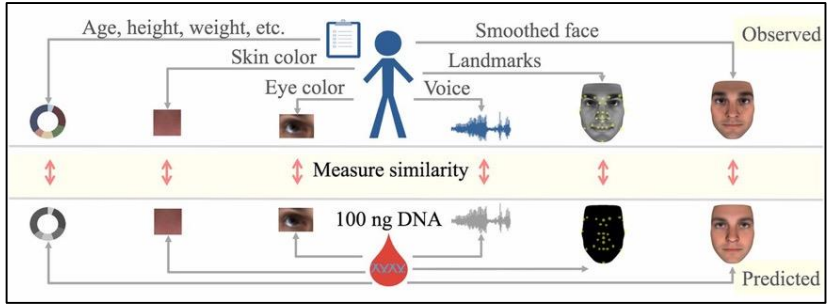
Homer et al. 2008 PLOS Genetics: aggregated genomic data (i.e., allele frequencies) can be used for re-identifying an individual in a case group with a certain disease

Gymrek et al. 2013 Science: surnames can be recovered from personal genomes, linking "anonymous" genomes and public genetic genealogy databases

Lipper et al. 2017 PNAS: Anonymous genomes can also be identified by inferring physical traits and demographic information



Standard de-identification and anonymization techniques are ineffective with genomic data



Data Protection in Personalized Health

P4 (Predictive, Preventive, Personalized and Participatory) medicine

- Revolutionize healthcare by providing better diagnoses and targeted preventive and therapeutic measures

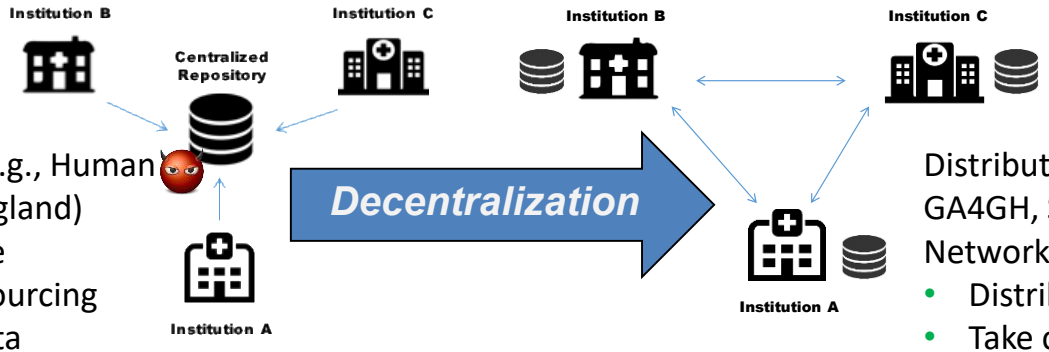
Technical Challenges:

- Interoperability
- Efficiency and usability in data sharing
- Scalability/Big Data
- Mitigation of privacy risks and compliance with data protection

Swiss Personalized Health Network

Strategic Focus Area
Personalized Health and Related Technologies

Centralized vs Distributed Approaches:



Centralized approach (e.g., Human Longevity, Genomics England)

- Single point of failure
- Impossibility of outsourcing individual patient data

Distributed approach (e.g., Beacon GA4GH, Swiss Personalized Health Network - SPHN)

- Distributed trust
- Take computation to the data

Technologies for Privacy and Security Protection

C4DT Center for Digital Trust

Traditional Encryption

- Protects data at rest and in transit
- Cannot protect computation

Homomorphic Encryption

- Protects computation in untrusted environments
- Limited versatility vs efficiency

Secure Multiparty Computation

- Protects computation in distributed environments
- High communication overhead

Trusted Execution Environments

- Protects computation with Hardware Trusted Element
- Requires trust in the manufacturer, vulnerable to side-channels

Differential Privacy

- Protects released data from inferences
- Degrades data utility (privacy-utility tradeoff)

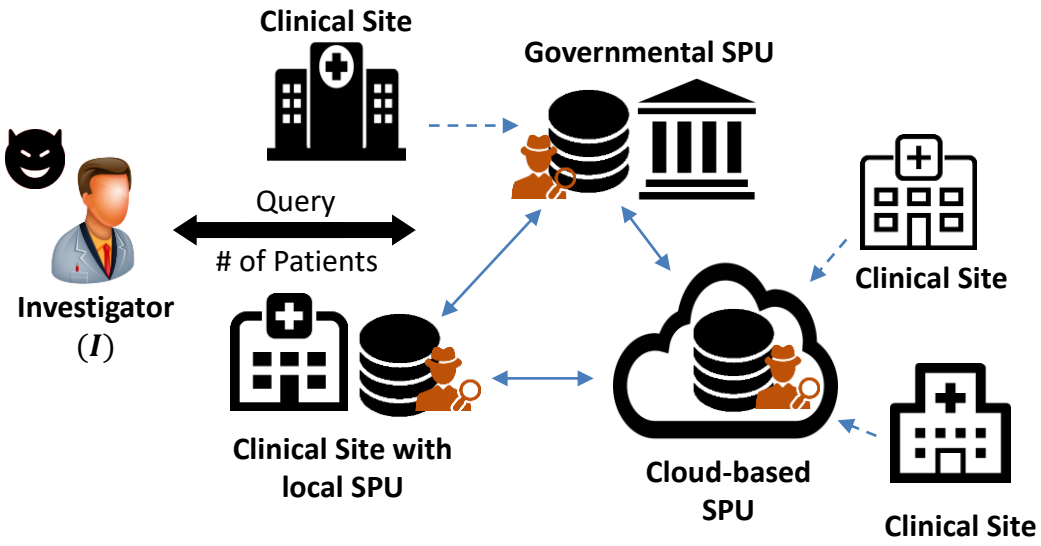
Distributed Ledger Technologies (Blockchains)

- Strong accountability and traceability in distributed environments
- No privacy by default

DPPH

EPFL

System and Threat Models



SPU: Storage and Processing Unit

Honest-but-curious adversary:

- honestly follows the protocol
- tries to infer sensitive data from the different steps of the protocol

Malicious-but-covert adversary:

- can tamper with the protocol
- tries to infer sensitive data from the query end-result

Main Privacy and Security Challenges

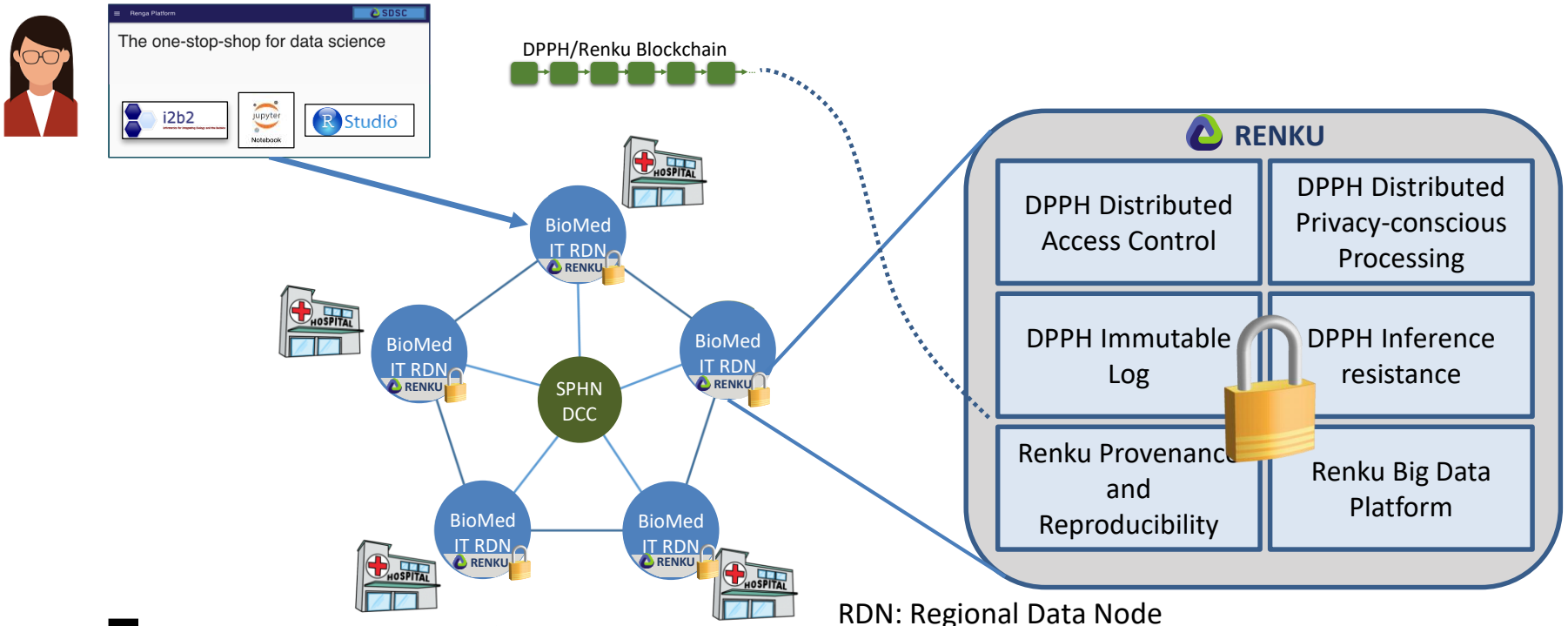
- **Loss of data confidentiality** due to illegitimate access to the data
  - External (hacker) or internal (insider) attacker stealing the data

➔ Standard encryption can protect data ONLY at rest or in transit BUT NOT during processing (e.g., in the memory)

- **Patient re-identification** due to legitimate access to the data
  - Malicious users performing "smart" data requests in order to re-identify patients in a specific dataset (e.g., patients with HIV)

➔ De-identification or anonymization is ineffective with genomic data

Envisioned Secure Infrastructure for Privacy-Conscious Medical Research in Switzerland



RDN: Regional Data Node
DCC: Data Coordination Center

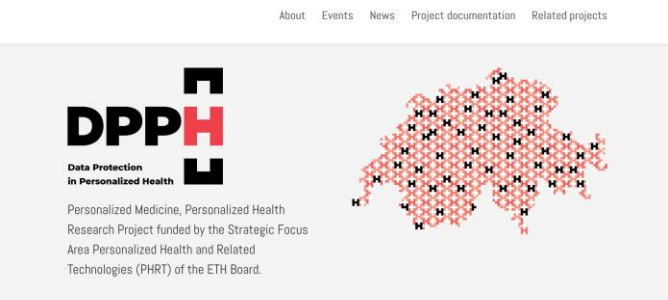
MedCo: Demo Video

Conclusions

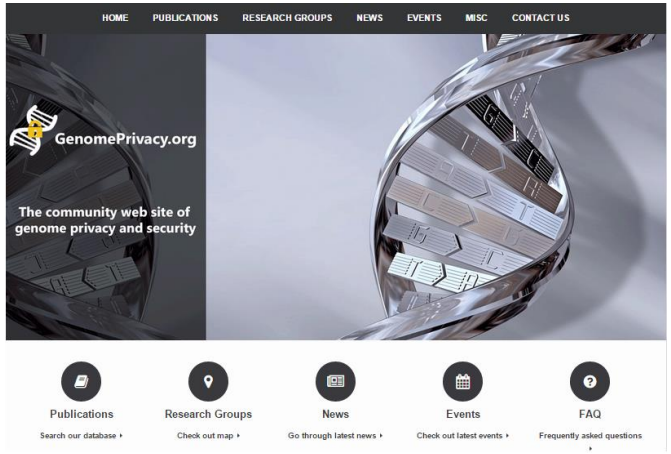
- Worldwide, the confidentiality of health data is **in jeopardy**
- Precision medicine dramatically **increases the amount of data**
- **Technology alone** will not solve the problem
- The ***Data Protection in Personalized Health*** Project is a (Swiss) response to these concerns

Useful Links and Further Information

https://dpph.ch



https://genomeprivacy.org



https://c4dt.org

https://medco.epfl.ch

Community website

- Searchable list of publications on genome privacy and security
- News from major media (from Science, Nature, GenomeWeb, etc.)
- Research groups and companies involved
- Tutorial and tools
- Events (past & future)

Liability, Privacy and Security in Medical Data Sharing: the Swiss Experience

Ria Kechagia
Juan Ramón Troncoso-Pastoriza

ria.kechagia@epfl.ch
juan.troncoso-pastoriza@epfl.ch