April 5, 2019

Anonymous and Pseudonymous Health Data: European and U.S. Perspectives

Elizabeth Canter
Covington & Burling LLP

Jennifer Chillas
Bristol-Myers Squibb Company

Thomas Steiner
VISCHER AG

International Privacy+ Security Forum

Agenda

- Introduction
- Value Proposition
- European Legal Landscape
- U.S. Legal Landscape
- Hypotheticals

Introduction

International
Privacy+
Security
Forum

Speaker

Elizabeth Canter

Partner

Covington & Burling LLP (Washington, D.C.)

- Privacy and data protection lawyer advising technology, life sciences, health and other companies
- Active in Firm's Digital Health, AI, and Internet of Things Initiatives

Speaker

Jennifer Chillas

Senior Corporate Counsel

Bristol-Myers Squibb Company (New York, NY)

- Advise on U.S. privacy law as well as digital and social media activities
- Formerly an associate with Ropes & Gray in Boston, Massachusetts
- Prior to law school, was a pharmaceutical chemist

Speaker

Thomas Steiner

Head of Data & Privacy Practice

VISCHER AG (Zurich, Switzerland)

- Data & privacy lawyer, advising companies on Swiss and EU data protection law
- Particular focus on regulated sectors in digital transformation, including health

Disclaimer

Our opinions are our own and not those of our firms, companies, or clients.

Purpose & Goals

- Consider how organizations can develop and deploy innovative products and services while complying with sometimes competing demands for the use of anonymous or pseudonymous health data in EU, Swiss and U.S. law
- Recognize differences in requirements for de-identification (i.e. anonymization or pseudonymization)
- Understand how – through anonymization and pseudonymization – companies can meet regulatory requirements while maintaining their competitive edge

Value Proposition

International
Privacy+
Security
Forum

Licensing De-identified Data

Example

- Pharmaceutical company licenses “de-identified” data
- Licensors may include: specialty pharmacies, electronic medical record companies, or others

Value Proposition

- Data support important analyses of patient adherence and value of patient support programs
- Real world evidence may support approval of new indications for approved drugs and to satisfy post-approval study requirements
- Data may also support marketing

Connected Devices

Example

- Medical device manufacturer establishes a cloud-based platform
- Information from connected devices and other sources can be analyzed by therapists and data scientists using platform

Value Proposition

- Device data has the potential to support development and improvement of devices and expansion of offerings
- Data analysis can also help tailor care to needs of patient

Collaborations Involving Genetic Data

Example

- Life sciences or digital health company seeks to conduct research on genetic data that was originally collected by another party

Value Proposition

- Genetics increasingly factor into diagnosis and treatment options
- This is "personalized" or "precision" medicine

European Legal Landscape

International Privacy+ Security Forum

Health Data Law (Switzerland)

- Fragmented legal landscape – example: Switzerland
- Sector-specific laws
  - Federal (e.g. Human Research Act / Human Genetic Testing Act)
  - Swiss States / Cantons (e.g. Cantonal Patients‘ / Health Acts)
- Physician-Patient-Privilege (criminal law provision)
- Social security laws
- General data protection laws (Federal, State / Cantons, and – where applicable – EU GDPR)

Personal Health Data

Personal Data	Individual is **identified** or (in combination with other information) **identifiable**	🔴
Pseudonymous Data	**Reversibly de-identified data:** information linked to pseudonymous code, re-identification possible and reasonably likely (using identification “key”) / remains “personal data” in most circumstances under EU GDPR	🔴🟡
Anonymous Data	**Irreversibly de-identified data:** re-identification not reasonably likely – requires extraordinary efforts, which no motivated / interested person would reasonably use	🟢

Health Data – Personal Data (Switzerland)

- Swiss Federal Supreme Court (cases *Logistep* and *Google Street View*) applies **relative approach** to identification
- Individual is **identifiable** using **additional information / knowledge** (circumstances, context)
- **Organization holding or receiving data** has **access** to required additional information / knowledge and **will reasonably likely use** this information in order to identify individual (considering time, costs, technical means)

Health Data – (reversible) de-identification

- Example: (Swiss) Human Research Ordinance regulating use of biological material / personal health data:
  - “anonymization”– identifying information needs to be “irreversibly” effaced or deleted
  - “correctly coded” (i.e. pseudonymous) if qualified as “anonymized” from the point of view of a person who has no access to the key
- Coded / pseudonymous data also referred to as **reversibly de-identified** (or factually anonymized) data

Anonymization Methods / Approaches

- Anonymization methods (selection)
  - Masking
  - Randomization
  - Data aggregation / generalization
- Approaches to anonymization of data sets
  - More ambitious technically: splitting at the source / near the data point (“edge”) – originally two separate data sets (one with anonymous data, one with identifying information)
  - More ambitious legally: copy data set – anonymize it

Health Data – Personal Data (EU GDPR)

- Consider additional information / knowledge if interested person would **reasonably likely** use it to (re-) identify individual
- Issue: need **illegal means** be considered?
  - Likely not, according to CJEU in *Breyer* and according to UK ICO‘s “motivated intruder” test;
  - Yes, according to some academics and (increasingly) data protection supervisory authorities, at least if readily and cheaply available (considering data breaches, in particular)

→ Data tied to pseudonymous codes (pseudonymized data) will in most circumstances remain personal data under EU GDPR (re-identification using “key” / code)

Personal Data Concerning Health

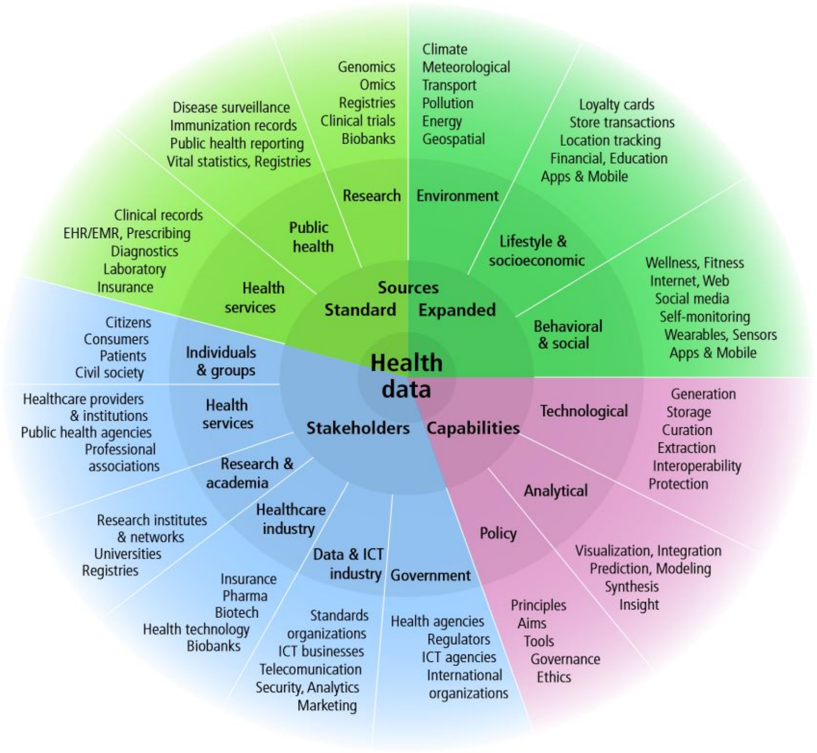
- Traditional: data that represents **medical diagnosis** with negative effect for individual concerned
- Evolving to broader conception: personal data revealing information relating to the **past, current or future physical or mental health status** of data subject (cf. Art. 4(15) and Recital 35 GDPR, CJEU in *Lindqvist*)
- Now includes information from testing of genetic data or biological samples, and any information on disease, disease risk, physiological or biomedical state – in each case **independent of source**, e.g. health professional or medical device (cf. GDPR, Recital 35)

Personal Data Concerning Health – Practical Relevance

- Special category of personal data, implications include (GDPR):
- Higher **data security** standards required (risk-based approach)
- Increased **information / transparency** requirements
- Explicit **consent** more likely required for lawful processing
- **DPIA, prior consultation**: more likely required (high risk)
- **Data breach notification** more likely required (high risk)
- **DPO** required if core activities involve large-scale processing
- Member States may, in **sector-specific laws** specify rules for the processing of personal data concerning health

Health Data Ecosystem (WHO)

Evolving health data ecosystem



E. Vayena, J. Dzenowagis, M. Langfeld, 2016

- Non-legal definition of health data
- Traditional: clinical records (e.g. medical history, diagnostics, treatment)
- New / expanding:
  - performance data from medical devices
  - data from *omics* studies
  - lifestyle and socioeconomic data
  - behavioral and social data
  - Quantified self (wearables & sensors)

Health Data – Big Data

- Large amounts of data, collected from different sources over a long period of time
- **Combination / correlation**: **socioeconomic, lifestyle, genomic** or **behavioral** data used to determine / predict – in particular, by means of **data analytics** – current or future (physical or mental) health status (personalized medicine / care)
- Legal certainty / enforceability: Necessary to **delimit** notion of "personal data concerning health" (e.g. in relation to Art. 4(15) GDPR)
  - Consider context: **health-related** use?
  - Consider purpose: **health-related** use intended?

U.S. Legal Landscape

HIPAA

- Applies only to covered entities and business associates
- Restricts use or disclosure of PHI except as permitted or required by HIPAA Privacy Rule
- Examples of permitted disclosures: for purposes of treatment, payment, or health care operations, certain enumerated public policy purposes, with the individual's written authorization

- Information is de-identified when either:
  - A person with appropriate expertise determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information; or
  - Safe Harbor: all identifying information has been removed

HIPAA Safe Harbor: 18 Direct Identifiers

- Names
- Geographic subunits smaller than a state
- All elements of date (except year)
- Telephone numbers
- Fax numbers
- E-mail address
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate / license numbers
- Vehicle identifiers and serial numbers (incl. license plates)
- Device identifiers and serial numbers
- URLs
- IP numbers
- Biometric identifiers (e.g., fingerprints)
- Full-face photographic images
- Any other unique identifying number, characteristic, or code

Federal Trade Commission Act

- Section 5 authorizes the Federal Trade Commission (FTC) to address “deceptive” or “unfair” acts or practices
- Key Section 5 themes:
  - No false or misleading statements about privacy practices
  - Disclose unexpected privacy practices
  - Obtain affirmative consent for material retroactive changes and unexpected practices involving sensitive information (including health information)
  - Maintain reasonable and appropriate information security safeguards

2012 FTC Privacy Report

"With improvements in technology and the ubiquity of public information, more and more data [can] be "reasonably linked" to a consumer, computer or device. . . To address this issue, the Report clarifies that data is not "reasonably linkable" to the extent that a company: (1) takes reasonable measures to ensure that the data is de-identified; (2) publicly commits not to try to re-identify the data; and (3) contractually prohibits downstream recipients from trying to re-identify the data."

California Consumer Privacy Act ("CCPA")

Opt-out of "Sale" (Opt-in for minors)

- "Sale" of personal information means processing "for monetary or other valuable consideration"

Data Access

- Can request access to "specific pieces of personal information," categories of information collected, categories of third parties who receive data, etc.

Data Portability

- When responding to a data access request, data must be provided in a portable and (where possible) readily useable format

Data Deletion

- Subject to a number of exceptions, must delete personal information and direct service providers to do the same

CCPA: Broadly Defines Personal Information

- **PI**: identifies, relates to, describes, is capable of being associated with, or could reasonably be linked with a particular consumer
- But no restriction on use or disclosure of data that is:
  - **De-identified**: cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked to a particular consumer; and controls prevent re-identification
  - **Aggregate**: relates to a group or category of consumers, from which individual consumer identities have been removed, that is not linked or reasonably linkable to any consumer or household
- Certain limited exceptions for "research" are tied to whether personal information is both de-identified and pseudonymized

State Genetic Privacy Laws

- There are a large number of state laws regulating use and disclosure of genetic information
- Majority of states require written consent from subject prior to disclosure of genetic information
- States are split on whether and how they restrict the future uses and disclosure of genetic information for research
  - Some states exempt certain kinds of anonymous data from state genetic privacy protections
  - But other states require individuals be provided right to opt in or out of research uses of data even if data is anonymized or coded

Hypotheticals

Licensing De-identified Data

- Pharmaceutical company licenses “de-identified” personal data from specialty pharmacy
- Specialty pharmacy uses a third party aggregator to de-identify personal data on its behalf

Licensing De-identified Data

U.S. and European Perspectives

- Specialty pharmacy is covered entity for purposes of HIPAA
  - Disclosure to third-party aggregator requires business associate agreement
  - Disclosure to pharmaceutical company typically limited to data that has been de-identified pursuant to aggregator's expert determination
- Even if data is de-identified for purposes of HIPAA, there may be FTC, CCPA, GDPR, sector-specific laws in relevant countries, or other implications if data remains reasonably capable of being linked to a particular individual or household / if re-identification is reasonably likely

Practical Tips

- Consider contractual allocation of risk as between specialty pharmacy, data aggregator, and pharmaceutical company
- In some cases, further due diligence may be appropriate
- Recipient of de-identified data may want to consider putting in place policies, procedures, or other controls to prevent risk of re-identification

Data From Connected Devices

- Medical device manufacturer will establish a cloud-based platform connecting medical devices (as well as health care professionals and their patients) for personalized care / therapy purposes
- Types of data: patient master data, patient condition data, medical data, and (automatically generated) device performance data
- Analysis and use of **separate, de-identified set of performance data** by medical device manufacturer / platform provider to gain insights on how to improve and further develop devices and platform

Data From Connected Devices

U.S. and European Perspectives

- Avoid application of privacy laws through de-identification
- Europe: De-identification using a combination of methods, including masking, randomization and data aggregation / generalization. Note: Higher degree of de-identification may lower quality of data set, but makes re-identification less likely
- U.S.: De-identification standards vary based on context

Practical Tips

- Legal engineering: Consider technical solution how to separate and de-identify data sets close to data point (edge computing)
- Implement technical and organizational security measures as well as contractual confidentiality obligations, which make it very unlikely that manufacturer / provider would re-identify data
- Implement contractual framework: allocating of roles, responsibilities

Collaborations Involving Genetic Data

- Multiple pharmaceutical companies enter research consortium that involves the sequencing of genomes
- Consortium members will get exclusive initial access to genetic data
- Information is tied to codes rather than more personal identifiers

Collaborations Involving Genetic Data

U.S. and European Perspectives

- Data tied to pseudonymous codes may remain personal data for purposes of data privacy laws
- Risk regulators could take position that genome sequences cannot by their nature be anonymized
- Even if truly anonymous, there may be obligations to obtain consent to use genetic information for secondary research purposes

Practical Tips

- Consider contractual allocation of risk as between entity that obtained consent for testing and use of genetic information and entity that will conduct research
- In some cases, further due diligence may be appropriate
- Recipient of genetic information may want to put in place controls, e.g., prevent use of data to develop a single person’s genomic sequence

Questions + Contact

Elizabeth Canter
Partner
Covington & Burling LLP
Washington, D.C.
ecanter@cov.com

Jennifer Chillas
Senior Corporate Counsel
Bristol-Myers Squibb
Company, New York, NY
jennifer.chillas@bms.com

Thomas Steiner
Head, Data & Privacy Practice
VISCHER AG
Zurich (Switzerland)
tsteiner@vischer.com