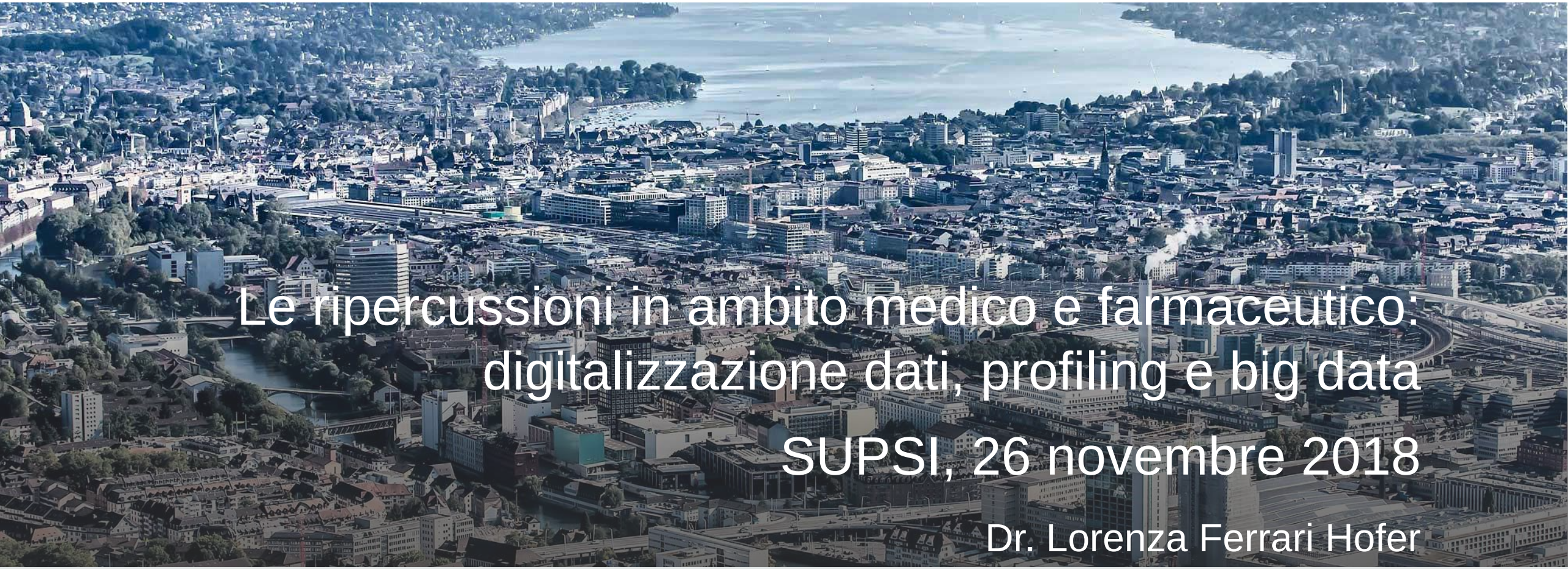
PESTALOZZI

ATTORNEYS AT LAW



Le ripercussioni in ambito medico e farmaceutico: digitalizzazione dati, profiling e big data

SUPSI, 26 novembre 2018

Dr. Lorenza Ferrari Hofer

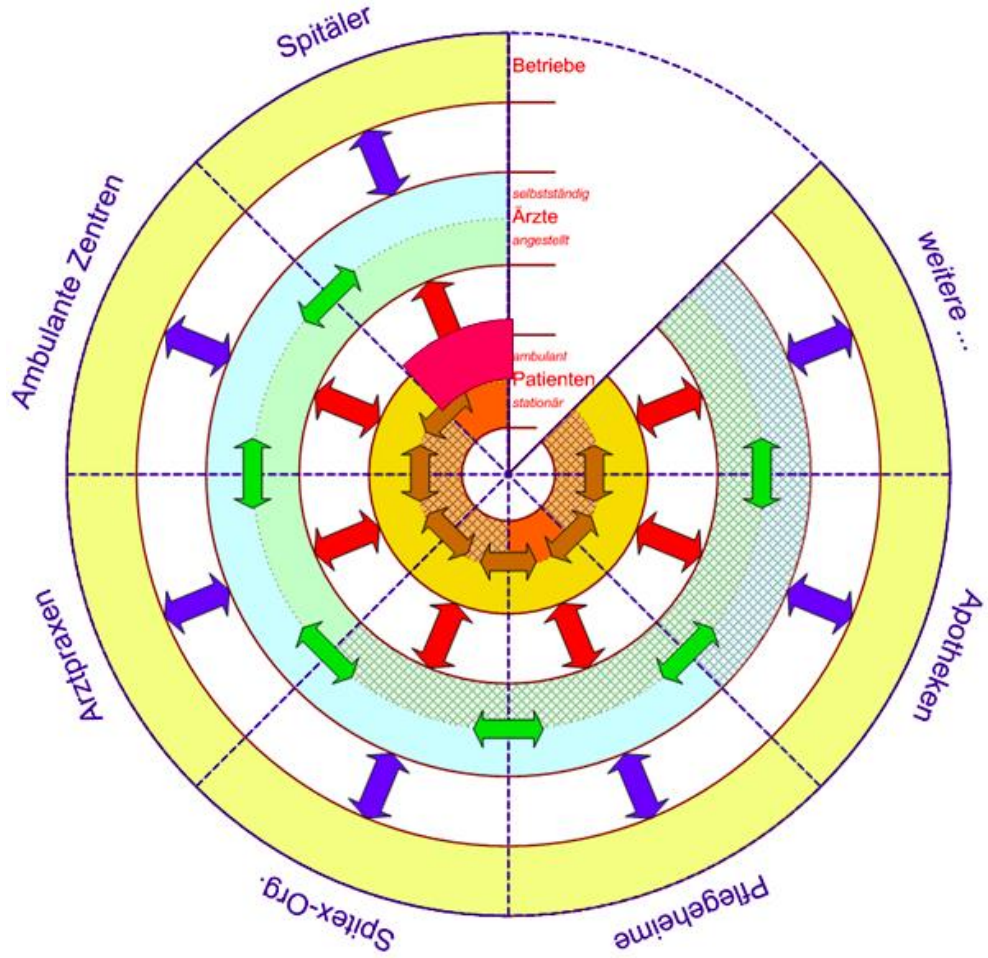
Introduzione

- Società digitale – nuove tecnologie portano nuove forme di comunicazione e di uso dei dati
- Crescente quantità di dati di provenienza diversa (Big Data)
- Analisi, trattamento e interazione tra i dati viene effettuata attraverso logoritmi, senza intervento umano (Intelligenza Artificiale)
- Diverse forme – dati formati da numeri e lettere, immagini, suoni e altri
- Diversi contenuti – dati tecnici, dati personali e altri

Dati in ambito medico e nella ricerca farmaceutica

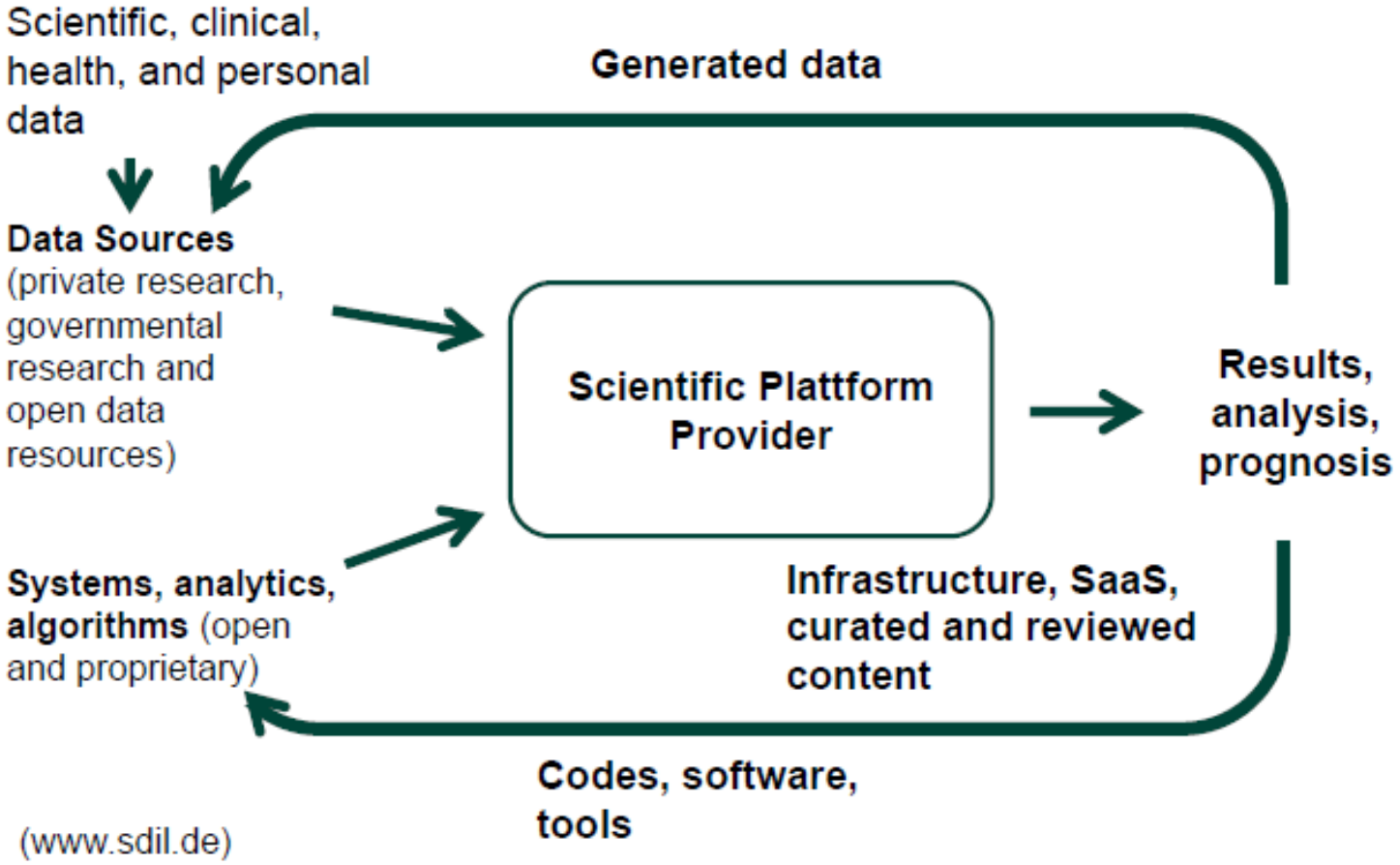
- Dati relativi a trattamenti medici, sostanze farmaceutiche
- Dati personali del personale specializzato, sponsors, ospedali, ecc.
- Dati personali dei patienti (identificabili)
  - Nomi, indirizzi, numero di telefono
  - indicazioni sulla salute, sullo stato della malattia
  - Indicazioni su famiglia, assicurazioni, ecc.
  - Dati genetici
  - Dati sanitari
  - Profiling (profilazione)
- Dati anonimi e pseudoanonimi
- Big data (Volume, Variety, Velocity, Value)

Utilizzo dati in ambito medico



Progetto MARS (trattamento dati statistici e amministrativi, prestazioni ambulatorie), Ufficio Federale Statistica, © 2013

Utilizzo dati nella ricerca farmaceutica



Basi legali CH / Disposizioni LPD

- Dati personali concernenti la salute o la sfera intima sono **dati personali degni di particolare protezione** (art. 3 lett. c LPD)
- Una compilazione di dati che permette di valutare le caratteristiche essenziali della personalità di una persona fisica sono **profilo della personalità** (art. 3 lett. d LPD)
- Obbligo di informazione (identità del detentore della collezione dati, finalità del trattamento dati, categorie dei destinatari) (art. 14 LPD)
- Divieto della comunicazione a terzi senza giustificazione (consenso, interesse preponderante privato o pubblico, legge) (art. 12 cpv. 2 lett. c LPD)
- Il consenso è valido soltanto se espresso liberamente e dopo debita informazione. Esso deve essere esplicito (art. 4 cpv. 5 LPD)
- Notificazione collezioni di dati (art. 11a cpv. 3 lett. a LPD)

Basi legali CH / Cartelle cliniche e dati medici

- LDP vale per tutte le cartelle cliniche redatte e i dati medici dei pazienti da **cliniche e medici privati**
- Autorità federali possono solo trattare dati personali se ciò è necessario (art. 21 LPD)
- Alle cartelle cliniche tenute da ospedali pubblici (cantonali) si applica la relativa legge cantonale (p.es. LPDP, LSan in Ticino)
- Medici e i dentisti, come pure gli ausiliari di questi professionisti, sono tenuti al segreto professionale (segreto medico, art. 321 CP)
- Flusso di dati medici tra assicurazioni (4A_294/2014), consegna rapporti di cura alle assicurazioni malattia
- SwissDRG – assicuratori malattia necessitano di un servizio di ricezione dei dati certificato (art. 59a OAMal)

Basi legali CH / Ricerca sull'essere umano

- La ricerca sull'essere umano può essere condotta soltanto se
  - (i) la persona interessata vi ha acconsentito
  - (ii) dopo essere stata sufficientemente informata, tra altri sulle misure destinate alla protezione dei dati personali raccolti,
  - (iii) dopo un congruo termine di riflessione.
  - (iv) Il consenso deve essere scritto (art. 7, 16 LRum)
- Consenso al trattamento dati non necessario per **dati medici anonimizzati o pseudonimizzati** (re-identificazione per terzi impossibile o possibile soltanto al prezzo di un enorme dispendio) (art. 25 ss ORum)

Normativa UE 2016/679 / GDPR

- **Liceità, correttezza, trasparenza** – i dati devono essere trattati in modo lecito, corretto e trasparente nei contronti dell'interessato
- **Limitazioni delle finalità** – i dati devono essere raccolti per finalità determinate, esplicite e legittime
- **Minimizzazione dei dati** – possono essere trattati solo dati necessari rispetto alle finalità
- **Esattezza** – i dati devono essere sempre esatti e aggiornati
- **Limitazione della conservazione –** i dati devono essere conservati sono per un arco di tempo necessario al conseguimento delle finalità
- **Integrità e riservattezza** – i dati devono essere trattati in maniera da garantire un'adeguata sicurezza, anche da atti illeciti e dalla perdita

Nuove definizioni GDPR

- **Dati relativi alla salute –** dati attinenti alla salute fisica e mentale di una persona fisica, compresi dati di servizi di assistenza sanitaria (art. 4 (15) GDPR)
- **Dati genetici –** (art. 4 (13) GDPR)
- **Profilazione** - trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti […] la salute, […] il comportamento (art. 4 (4) GDPR)
- **Pseudonimizzazione** - Trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti senza l'utilizzo di informazioni aggiuntive; le informazioni aggiuntive devono essere conservate separatamente e soggette a misure che garantiscono la non identificazione (art. 4 (5) GDPR)

Obblighi di informazione GDPR

- **Contenuto –** identificazione del titolare del trattamento, del responsabile del trattamento, delle finalità del trattamento, dei destinatari dei dati, durata del trattamento, attività di profiling
- **Diritti di informazione dell'interessato** - accesso ai dati, richiesta dati, rettifica e cancellazione, limitazione del trattamento, trasferibilità dati, reclamo ad un'autorità di controllo
- **Tempistica –** informazione al momento in cui i dati sono ottenuti
- **Responsabilità del titolare del trattamento –** misure tecniche (banche dati) e organizzative (processi, sorveglianza, ecc.) adeguate per garantire, ed essere in grado di dimostrare, il trattamento lecito (art. 24 (1) GDPR)

Consenso GDPR

- **Divieto di trattare dati della salute – consenso è eccezione** (art. 9 (1) GDPR)
- **Consenso –** manifestazione di volontà libera, specifica, informata e inequivocabile (art. 4 (11) GDPR)
- **«Informed consent» –** l'informazione concerne tutti i diritti dell'interessato e sul trattamento deve necessariamente precedere il consenso
- **Libero consenso –** l'esecuzione di un contratto non deve essere condizionata da un consenso trattamenti dati non necessario (art. 7 (4) GDPR)
- **Esplicito consenso –** per una o più finalità definite (art. 9 (2) (a) GDPR)
- **Revoca del consenso –** in qualsiasi momento e con la stessa facilità dell'accordo (art. 7 (3) GDPR)
- **Dimostrazione del consenso –** da parte del titolare del trattamento (art. 7 (1) GDPR)

Conseguenze per il trattamento in ambito medico e per la ricerca scientifica / UE

- **Pseudonimizzazione** – il trattamento ulteriore non deve più consentire di identificare l'interessato (art. 89 (1) GDPR)
  - Cambiamento di paradigma?
  - Anonimizzazione «di fatto» (identificazione solo con sforzo sproporzionato) non più possibile (art. 29 WG)
  - Deroghe «per finalità di interesse pubblico», praticamente non esistenti per il settore privato
- **Introduzione nuove norme specifiche sul consenso –** disposizioni limitative all'utilizzo dei dati medici e della salute, nuovi formulari
- **Introduzione responsabilità del titolare e del responsabile del trattamento** – sia sponsor che investigatori possono essere considerati titolari del trattamento (art. 5 (2) GDPR)

Conseguenze per il trattamento in ambito medico e per la ricerca scientifica / UE

- **Ricerca scientifica a fini propri** – non direttamente trattata dal GDPR, richiede ora una base legale e l'osservanza dei principi GDPR
- **Ricerca successiva su dati esistenti** – solo se si rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità specifiche e solo prendendo misure di protezione dati necessarie. Alternativa, con consenso
- **Trattamento transfrontaliero –** vale per studi scientifici multi-centers (?), per sponsors stranieri e per ospedali e cliniche che offrono attivamente prestazioni mediche a patienti residenti nell'UE
- **Nessuna regola di transizione –** vale anche per studi di ricerca già iniziati
- **https://www.cnil.fr/fr/sante**, altri organi nazionali

D-LPD

- Applicazione solo ai **dati personali di individui**
- Nessuna regola aggiuntiva per il trattamento dei dati della salute prevista, precisazione dei dati genetici (art. 4 lett. c D-LPD)
- Maggiore **trasparenza e informazione** per la persona interessata (art. 5 D-LPD)
- Nuove **responsabilità per il titolare del trattamento –** l'obbligo della protezione dei dati fin dalla progettazione (by design) e per impostazione predefinita (by default), obblighi di informazione e valutazione d'impatto (art. 6, 17-20 D-LPD)
- Adeguatezza dei **provvedimenti di protezione –** (art. 6 cpv. 2 D-LPD)
- **Espresso consenso** – consenso necessario, non necessariamente scritto (art. 5 cpv. 6 D-LPD)
- Introduzione definizione **profilazione –** simile a normativa UE (art. 4 lett. f D-LPD)

Conseguenze per il trattamento in ambito medico e per la ricerca scientifica / CH

- **Codici di condotta per ospedali –** sono in discussione e verranno presentati presto per approvazione alle autorità (art. 20 cpv. 5 D-LPD)
- **Consulente per la protezione dati –** nomina di fatto necessaria per attuare le responsabilità del titolare del trattamento (art. 9 D-LPD)
- **Responsabilità penale dei quadri ospedalieri –** art. 54 ss D-LPD
- **Registro delle attività di trattamento** – categorie delle persone interessate e dei dati, destinatari, durata di conservazione, descrizione dei provvedimenti, dati comunicati all'estero (art. 11 D-LPD)
- Dati delle **persone decedute –** art. 16 D-LPD
- **Notifica violazione** della sicurezza – art. 22 D-LPD
- Diritto **all'accesso della cartella clinica –** art. 23 D-LPD

Conseguenze per il trattamento in ambito medico e per la ricerca scientifica / CH

- **Anonimizzazione / pseudonimizzazione**, nella ricerca scientifica i dati degni di particolare protezione devono comunicati a terzi in una forma che non permetta d'identificare le persone interessate (art. 27 cpv. 2 lett. e, art. 35 cpv. 1 lett. a D-LPD)
- **Swissethics** – applicazione principi GDPR non necessaria; se le informazioni secondo GDPR sono fornite ai partecipanti, tali informazioni devono essere inoltrate alla commissione etica come addendum, ma solo per informazione e non per approvazione (www.swissethics.ch)

In sintesi …

- Sia GDPR che D-LPD richiedono misure aggiuntive per la protezione dei dati medici e riguardanti la salute, anche per la ricerca farmaceutica
- Particolare attenzione deve essere data al «profiling» nella ricerca farmaceutica
- Informazione e consenso sono richiesti per tutti i trattamenti di dati riguardanti la salute
- La nuova definizione di pseudonimizzazione nella GDPR richiede una modifica sostanziale delle procedure di consenso nella ricerca scientifica e farmaceutica
- GDPR non è applicabile in Svizzera, ma si raccomanda agli sponsor svizzeri di adattare le misure di protezione per ogni studio multi-center che coinvolge anche centri europei

Lorenza Ferrari Hofer

Partner
Head IP&TMT, Co-Head Life Sciences

Pestalozzi Attorneys at Law Ltd
Loewenstrasse 1
8001 Zurich, Switzerland
+41 44 217 92 57
lorenza.ferrari@pestalozzilaw.com

Grazie per la Vostra attenzione!

PESTALOZZI

ATTORNEYS AT LAW

Zurich Office

Pestalozzi Attorneys at Law Ltd
Loewenstrasse 1
8001 Zurich
Switzerland

T +41 44 217 91 11
F +41 44 217 92 17

Geneva Office

Pestalozzi Attorneys at Law Ltd
Cours de Rive 13
1204 Geneva
Switzerland

T +41 22 999 96 00
F +41 22 999 96 01