

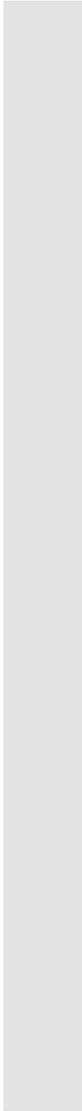


Data sharing and privacy: fatal attraction

Michele Scandola

Department of Human Sciences
University of Verona



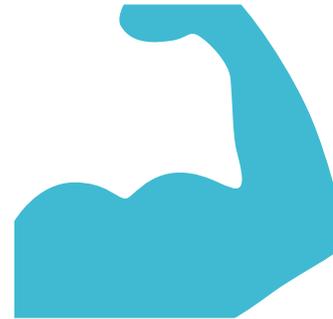


Introduzione

Cosa è uno studio MULTILAB?



Collaborazione
fra più laboratori



Replicabilità e
robustezza



Scalabilità



Condivisione dei
dati

Cosa è uno studio MULTILAB?



Collaborazione
fra più laboratori



Replicabilità e
robustezza

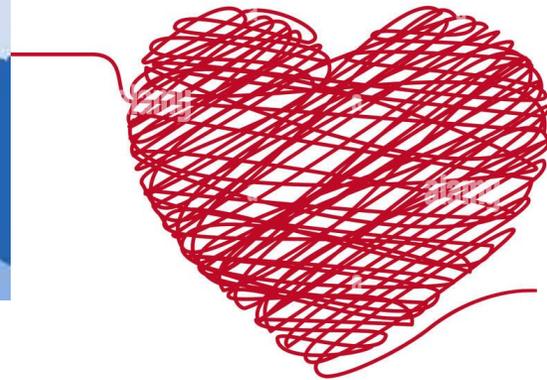
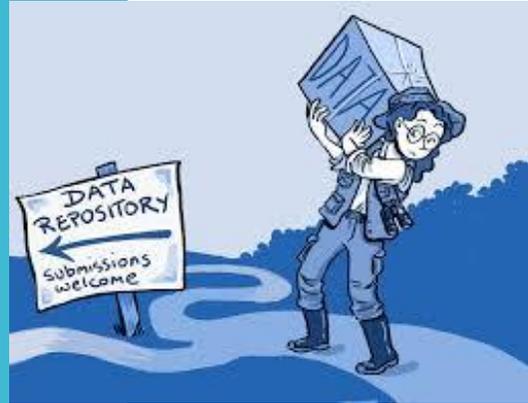


Scalabilità



Condivisione dei
dati

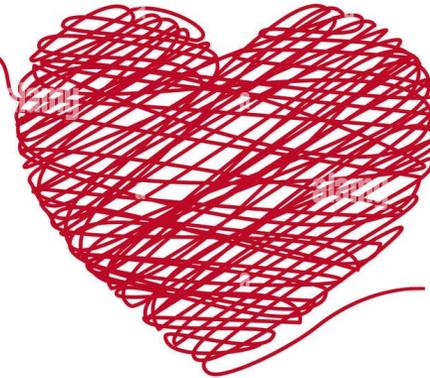
Abbiamo a cuore i nostri dati...



alamy

Image ID: D1F8TA
www.alamy.com

Abbiamo a cuore i nostri dati...

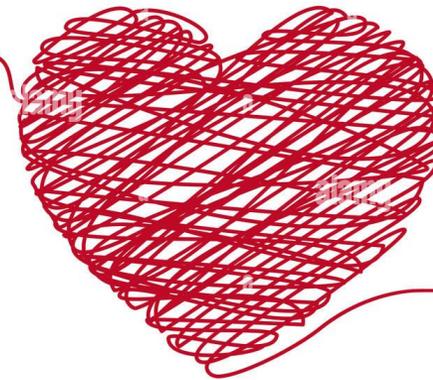


alamy

Image ID: D2F8TA
www.alamy.com



Abbiamo a cuore i nostri dati...



it's complicated

alamy

Image ID: D2F8TA
www.alamy.com



Come conciliare
Open Data in uno
studio MultiLab e le
leggi della privacy
dei diversi paesi?





GDPR e HIPAA

GDPR

- Tratta di dati di cittadini europei
- Si applica a tutti i dati personali, inclusi quelli sanitari
- Si basa su principi ampi e richiede il consenso esplicito

HIPAA

- Tratta di dati sanitari di cittadini statunitensi
- Si applica ad i dati sanitari come storia clinica, fatture mediche, dati identificativi
- Tratta della sicurezza e privacy dei dati sanitari

General Data Protection Regulation



- Consenso esplicito & Interesse pubblico o scientifico (Art. 6 e 9)
- Minimizzazione dei dati (Art. 5 e 6)
- **Anonimizzazione e pseudonimizzazione (Art. 32 e 89)**
- Diritti degli interessati (Art 12-23)
- **Conservazione dei dati (Art. 5 e 89)**
- Responsabilità e documentazione (Art. 30 e 5)
- Consenso informato (Art. 7 e 9)

Health Insurance Portability and Accountability Act



- Autorizzazione del partecipante / Esenzioni all'autorizzazione
- Set di dati limitato
- **Anonimizzazione e pseudonimizzazione**
- Protezione dei Dati Sanitari Protetti
- **Conservazione dei dati**
- Uso secondario dei dati
- Valutazioni di sicurezza e monitoraggio



**Coordinazione tra laboratori
di diversi paesi**

problemi di conformità



**Trasferimento internazionale
di dati**

restrizioni e deroghe



**Gestione del consenso
informato tra vari laboratori**



Data minimization

condivisione delle informazioni essenziali

Problemi da affrontare

Soluzioni

Nominare un Data Protection Officer (DPO)

Il suo compito è quello di garantire che il trattamento dei dati personali avvenga in conformità col GDPR e altre normative

- Supervisione della conformità
- Coordina il **Data Protection Impact Assessment**
- Definisce e monitora i **Data Sharing Agreements** e i **Data Processing Agreements**
- Gestione dei consensi
- Formazione e sensibilizzazione
- Audit e Monitoraggio Continuo
- Gestione delle Violazioni di Dati
- Interfaccia con le Autorità di Controllo
- Garantisce i diritti dei partecipanti agli studi

Soluzioni

il Data Processing and Sharing Agreement

Data Processing

- Raccolta, registrazione dati
- Organizzazione, strutturazione
- Variazione, adattamento o modifica
- Estrazione, consultazione, uso (i.e. l'impiego)
- Comunicazione o diffusione dei dati
- Raffronto o interconnessione
- Limitazione, cancellazione o distruzione

- Identificazione delle parti coinvolte – responsabilità correttamente attribuite e riconoscibili
- Definizione dello scopo del data sharing e le sue basi legali
- Oggetto e durata del trattamento
- Diritti, obblighi e funzioni delle parti
- Misure di sicurezza e protezione dei dati
- Conservazione e cancellazione dei dati

Soluzioni

Misure tecniche e organizzative per proteggere i dati

- Crittografia
- Pseudonimizzazione
- Controllo degli accessi:
 - Accesso basato sui ruoli
 - Autenticazione a più fattori
 - Registro degli accessi
- Monitoraggio continuo e revisione della sicurezza
 - Audit periodici
 - Aggiornamento delle misure
- Gestione delle violazioni di dati
 - Piano di risposta alle violazioni
 - Procedura di notifica

Soluzioni

Data Protection Impact Assessment (DPIA) – Art. 35

Necessario se dati personali «ad alto rischio»

Razza o etnia

Affiliazioni o credenze religiose, politiche o filosofiche

Genetici o biometrici per identificazione univoca

Dati inerenti la salute

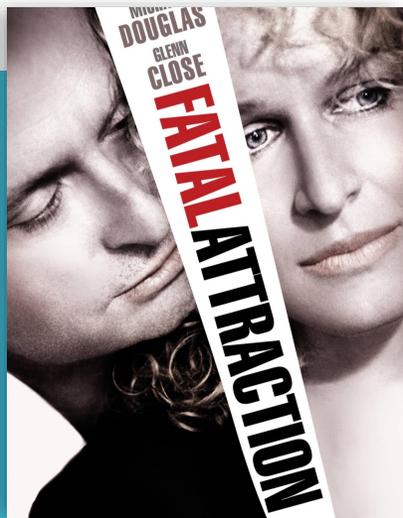
Dati inerenti la vita sessuale o orientamento sessuale

Dati che potrebbero avere conseguenze legali sui partecipanti

Dati inerenti a bambini

Dati che potrebbero portare a danno fisico ai partecipanti se trapelano

- Il DPIA contiene:
 - Una descrizione sistematica del processo di trattamento dei dati e del legittimo interesse del controllore dei dati
 - Una valutazione della necessità e adeguatezza delle operazioni sui dati in base agli scopi dello studio
 - Una valutazione dei rischi ai diritti dei partecipanti allo studio
 - Misure previste per affrontare i rischi
 - Misure di sicurezza
 - Risk Analysis



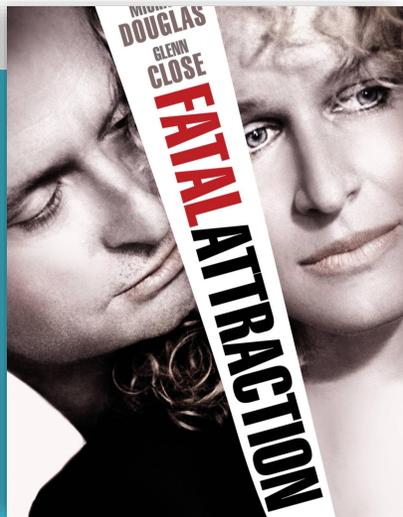
Soluzioni

Considerare il “livello di rischio” dei propri dati

Dati sull'infedeltà coniugale all'interno di un campione di convenienza (IRCSS) e specifica religione (es: valdese)

Dati sull'infedeltà coniugale all'interno di un campione di convenienza (es: dipendenti di un'IRCSS)

Dati sull'infedeltà coniugale da questionario online senza dati identificativi



Soluzioni

Considerare il “livello di rischio” dei propri dati

Dati sull'infedeltà coniugale all'interno di un campione di convenienza (IRCSS) e specifica religione (es: valdese)

Dati sull'infedeltà coniugale all'interno di un campione di convenienza (es: dipendenti di un'IRCSS)

Dati sull'infedeltà coniugale da questionario online senza dati identificativi

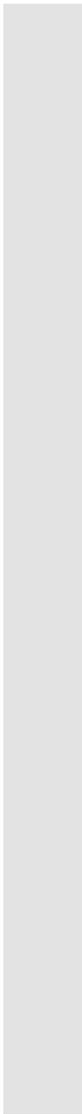
Dati sull'infedeltà coniugale all'interno di un campione di convenienza (IRCSS) e specifica religione (es: valdese)

Dati su stress ed ansia di un campione di convenienza (IRCSS) e specifica religione (es: valdese)

RTs a flanker task all'interno di un campione di convenienza (IRCSS) e specifica religione (es: valdese)

Soluzioni Amnesia

- Pseudonimizzazione
- Masking
- K-anonymity e K^m -anonymity
- **Demographic statistics**



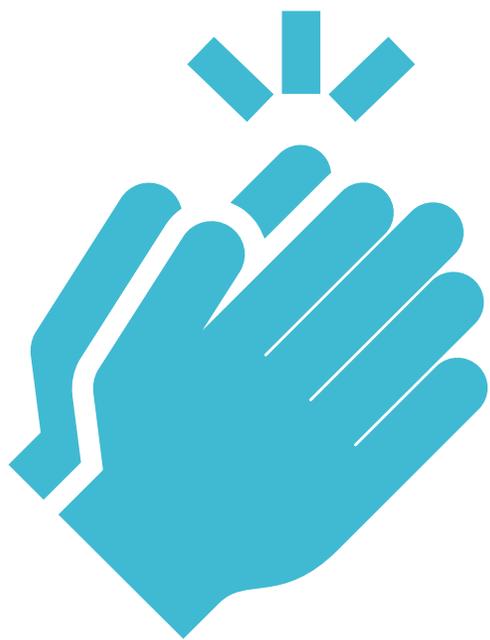
Considerazioni finali

Considerazioni finali

- La difficile corsa all'anonimizzazione...
- Considerare il «livello di rischio» dei propri dati
- Controllare e ricontrollare di aver minimizzato i dati
- Informare i partecipanti e far firmare consensi separati: allo studio, alla privacy, al data-sharing multilab, al data-sharing open data
- Nella condivisione dei dati in formato Open, assicurarsi dei possibili secondi fini
- Nominare un Data Protection Officer
- Formarsi e formare

ITRN Data Sharing Working Group

- **Giorgio Arcara** - IRCCS San Camillo Venezia, Venezia
- **Bonaria Biancu** – Università Milano-Bicocca, Milano
- **Marta Bortoletto** - IRCCS Istituto Centro San Giovanni di Dio Fatebenefratelli, Brescia, Italy
- **Antony Casula** - Dipartimento di Scienze Cognitive, Psicologiche, Pedagogiche e Studi Culturali (COSPECS), Università degli Studi di Messina, l'International School of Advanced Studies (ISAS), Università di Camerino
- **Vittorio Iacovella** - Centro Interdipartimentale Mente/Cervello, Università di Trento, Trento
- **Gian Mauro Manzoni** - Department of Brain and Behavioral Sciences, University of Pavia, Pavia
- **Paulo Santos** - IRCCS San Camillo Venezia, Venezia
- **Michele Scandola** - Dipartimento di Scienze Umane, Università di Verona
- **Marco Zanon** - Scuola Internazionale Superiore di Studi Avanzati, Trieste



Grazie a tutti per la vostra attenzione!

Website: michelescandola.netlify.app

Twitter/X account: @Scandle

Email: michele.scandola@univr.it