

CLOUD COMPUTING E SANITA'

Aspetti legati alla protezione dei dati personali

Lucio **Scudiero** LL.M., Membro del C.D.A.

Istituto Italiano Privacy – piazza San Salvatore in Lauro, 13 – 00186 Rome – Italy

l.scudiero@gmail.com - www.istitutoitalianoprivacy.it



L'Istituto Italiano per la Privacy e la Valorizzazione dei Dati (IIP) è un centro di ricerca e di advocacy finanziato solo da soggetti privati (persone fisiche, associazioni, studi legali e aziende anche multinazionali) dedicato alle tematiche della protezione e della valorizzazione dei dati personali, dell'informazione e dell'identità nella società globale dell'ICT.

L'Istituto coinvolge e mette in relazione molti tra i migliori specialisti italiani del diritto della privacy ma anche significativi rappresentanti degli ambiti pubblici e privati che con i dati personali, spesso sensibili, lavorano quotidianamente.

Operando come think tank, l'IIP è punto di riferimento per gli esperti italiani del “nuovo diritto” e per i diversi player dei mercati ad elevato contenuto tecnologico.

L'Istituto utilizza come principali strumenti di azione il sito internet, dove vengono pubblicati i contributi dei propri Soci Fellow e di altri ricercatori, e una **newsletter informativa quindicinale** con le principali notizie e analisi sulle evoluzioni delle problematiche privacy in Italia e nel mondo.

Si organizzano con frequenza trimestrale **convegni aperti al pubblico e workshop seminariali a porte chiuse**, dove possibile in partnership con realtà universitarie nazionali ed europee, per favorire la formazione dei professionisti e insieme per sensibilizzare i non addetti ai lavori, siano essi operatori di mercato o istituzioni pubbliche: tali incontri vengono sempre trasmessi anche in web-tv e web-radio, attraverso il portale dell'Istituto, e resi disponibili per il download o per la visualizzazione in modalità streaming.



STRUTTURA DELLA PRESENTAZIONE

1. ASPETTI GENERALI DI PROTEZIONE
DEI DATI
2. ASPETTI SPECIFICI DELLA SANITA' DI
PROTEZIONE DEI DATI



Alcuni documenti ufficiali pubblicati

- Art.29WP Parere 05/2012 su Cloud Computing
- European Cloud Strategy
- Linee di indirizzo nazionale sulla Telemedicina
- Linee guida in tema di Fascicolo Sanitario Elettronico e dossier sanitario
- Carta di Castelfranco per l'adozione del cloud in sanità
- Linee guida AgID per la presentazione di progetti regionali per il FSE (31 marzo 2014)
- Primo D.p.c.m. Attuativo FSE (Ex comma 7, art. 12 d.l. 179/2012) ??

CLOUD COMPUTING: problematiche generali

- Legge applicabile & giurisdizione
- Allocazione delle responsabilità
- Modifica dei termini/parti
- Portability / migration / transfer back vs. lock-in
- Termination
- SLAs + PLAs
- Trasferimento dati extra UE



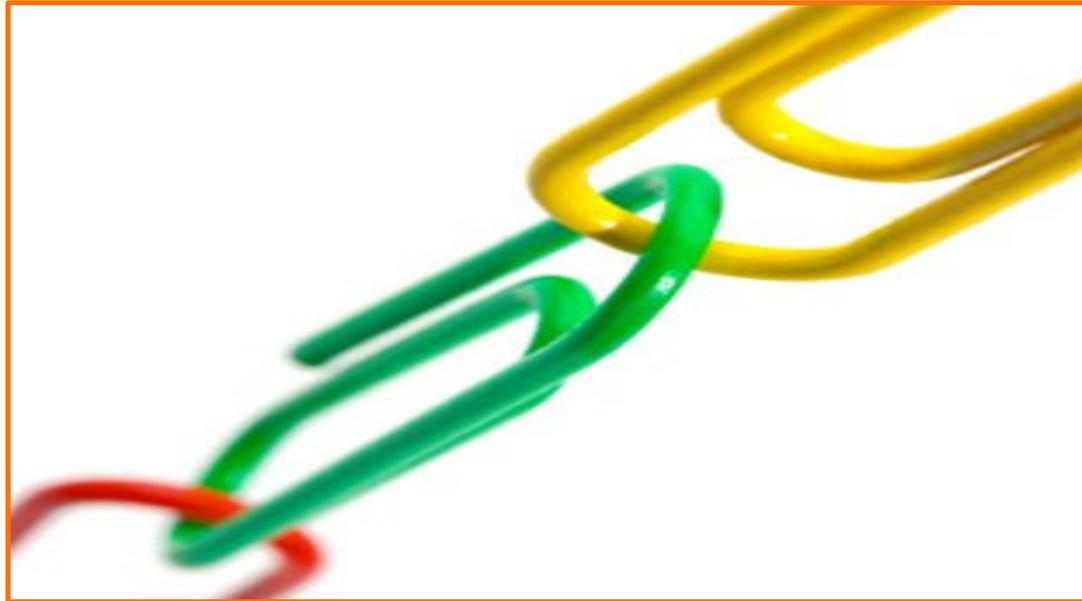


Legge applicabile & Giurisdizione





Allocazione delle responsabilità





Variazioni & Emendamenti contrattuali





Vendor Lock-in & Portability





Terminazione





Service Level Agreement & Privacy Level Agreement





CLOUD COMPUTING: problemi specifici nel settore sanitario



- Privilegiare il **Private cloud**
- **Normativa speciale per contratti con P.A.** (CAD e d.lgs. 12 aprile 2006 n. 163 - Codice dei contratti pubblici)
- **Misure di sicurezza** specifiche
- Normativa restrittiva in tema di **trasferimenti alla nuvola di dati sanitari**
- **Continuità operativa e disaster recovery**



Dati sensibili

- Tutti i dati personali nelle CCE sono sensibili. WP29, Documento di lavoro sul trattamento dei dati personali relativi alla salute contenuti nelle cartelle cliniche elettroniche (CCE) del 15 febbraio 2007: *“I membri del Gruppo di lavoro ritengono quindi che tutti i dati contenuti nella documentazione medica, nelle cartelle cliniche elettroniche e nei relativi sistemi debbano essere considerati “dati personali di natura delicata” -->> Consenso dell’interessato sempre necessario per trasferimento di dati fuori UE*



Cifratura dei dati sensibili

Cifratura dei dati sensibili. E.g. Codice della Privacy, Articolo 22 (6): *" I dati sensibili e giudiziari contenuti in elenchi, registri o banche di dati, tenuti con l'ausilio di strumenti elettronici, sono trattati con tecniche di cifratura o mediante l'utilizzazione di codici identificativi o di altre soluzioni che, considerato il numero e la natura dei dati trattati, li rendono temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità. "*

Misure di sicurezza per il trattamento di dati sensibili per mezzo di strumenti elettronici :

Articolo 34 (1) h) del Codice Privacy: *"adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari."*



Potenziali Criticità

- Trattamento di dati genetici;
- No CCE fuori-UE senza il consenso dell'interessato;
- Non ricorrere a soluzioni di public cloud per attività “mission critical” (meglio adottare soluzioni cloud ibride o private);
- Attenzione alla catena di IT sub-contractors.
- Riutilizzo dei programmi informatici realizzati su committenza delle Pubbliche amministrazioni



Strumenti specifici di sanità elettronica

- Fasciolo Sanitario Elettronico e Dossier Sanitario
- Telemedicina
- Applicativi d'uso comune (Prenotazioni, Registri, Riepiloghi/Report, Immagini, Documenti Clinici, Pratiche)



Conclusioni



ISTITUTO ITALIANO PRIVACY

○ Grazie per la vostra attenzione!

Lucio Scudiero, LL.M.

Membro C.d.A. – Istituto Italiano Privacy

l.scudiero@gmail.com

www.istitutoitalianoprivacy.it