Società Italiana
Telemedicina @ Sanità Elettronica

ORDINE AVVOCATI DI ROMA

Convegno di studio su
Privacy e Telemedicina

"Tra diritto del paziente alla riservatezza ed utilità della condivisione del dato sanitario"

IL NUOVO REGOLAMENTO PRIVACY DELL'UNIONE EUROPEA.
LE PRINCIPALI INNOVAZIONI IN MATERIA DI E-HEALTH

MARIA GABRIELLA VIRONE

AVVOCATO – PHD. IN DIRITTO E NUOVE TECNOLOGIE

Roma, 21 ottobre 2014

Sala Conferenze di Piazza Monte Citorio, 123/a

Agenda

- Background;
- Mutamento di scenario;
- Regolamento generale sulla protezione dei dati: principali innovazioni in materia di e-Health;
- Riflessioni finali.

Origini della protezione dei dati personali

Il "diritto alla protezione dei dati personali" è un diritto fondamentale, distinto ma strettamente legato al "diritto al rispetto della vita privata e familiare"

(cfr. artt. 7 e 8 della **Carta dei diritti fondamentali dell'Unione Europea**)

Verso l’armonizzazione delle leggi nazionali

Ad oggi, **pietra miliare** della normativa europea in materia di protezione dei dati è la **direttiva 95/46/CE** che disciplina la tutela delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati.

Implementata nelle legislazioni nazionali, la Direttiva si applica in tutti gli Stati membri dell'UE nonché in Islanda, Liechtenstein e Norvegia.

Mutamento di scenario

L'uso delle **Tecnologie dell'Informazione e Comunicazione** ha, tra gli altri, determinato:

- la definizione di nuovi modelli organizzativi aziendali,
- nuove **modalità di raccolta e di fruibilità dei dati**,
- la diffusione di **forme digitali per la memorizzazione dei dati sensibili**,
- il **trasferimento crescente di dati personali attraverso le frontiere nazionali, interne ed esterne**

Criticità

Le disposizioni vigenti non hanno impedito la **frammentazione** delle modalità di applicazione della protezione dei dati personali nel territorio dell'Unione, né ha eliminato l'**incertezza giuridica** e la diffusa percezione nel pubblico che le operazioni on line comportino notevoli **rischi**

(cfr. First report on the implementation of the Data Protection Directive (95/46/EC), 15.5.2003, COM (2003) 265 final; Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive (2007/C 255/01); Speciale Eurobarometro (EB) 359, Data Protection and Electronic Identity in the EU (2011))

Effetti del Trattato di Lisbona

L'articolo 16, parr. 1 e 2, del **Trattato sul funzionamento dell'Unione europea** riconosce il "diritto alla protezione dei dati personali" e assegna al Parlamento ed al Consiglio il compito di adottare norme in materia di protezione dei dati personali secondo la procedura legislativa ordinaria

Nuovi obiettivi dell'Unione europea

Istaurare un clima di **fiducia** dei consumatori:

- definendo una **politica forte e coerente** in materia di protezione dei dati personali,
- predisponendo un **quadro giuridico comunitario più solido e "globale"**, idoneo alle sfide delle nuove tecnologie

(cfr. Communication from The Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, A comprehensive approach on personal data protection in the European Union, Brussels, 4.11.2010, COM(2010) 609 final)

Il Regolamento Generale sulla Protezione dei Dati

Proposta di **Regolamento** del parlamento europeo e del consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati), Bruxelles, 25.1.2012, COM(2012) 11 def.

"Nel definire le norme tecniche e le misure organizzative atte a garantire la sicurezza del trattamento, la Commissione deve promuovere la **neutralità tecnologica**, **l'interoperabilità** e **l'innovazione** e, ove opportuno, la **cooperazione** con i paesi terzi" (cfr. Considerando 66).

Principali innovazioni in materia di e-Health

- Ambito di applicazione: anche al trattamento dei dati personali interamente o parzialmente **automatizzato** e non automatizzato (ex art. 2, co. 1)

↓

Necessità di formazione degli operatori socio-sanitari in termini conoscenze e competenze sulle regole del trattamento automatizzato dell'informazione

- Regole **univoche** sulla protezione dei dati personali nei 28 Paesi membri dell'Unione europea (ex art. 3)

↓

Benefit anche sul fronte del contenzioso

- **Dimensione internazionale** della protezione dei dati (ex art. 3)

"1. Il presente regolamento si applica al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento di un responsabile del trattamento o di un incaricato del trattamento **nell'Unione**.

2. Il presente regolamento si applica al trattamento dei dati personali di residenti nell'Unione effettuato da un responsabile del trattamento che **non è stabilito nell'Unione**, quando le attività di trattamento riguardano:

a) l'offerta di **beni** o la prestazione di **servizi** ai suddetti **residenti** nell'Unione, oppure

b) il **controllo** del loro comportamento.

3. Il presente regolamento si applica al trattamento dei dati personali effettuato da un responsabile del trattamento che **non è stabilito nell'Unione, ma in un luogo soggetto al diritto nazionale di uno Stato membro in virtù del diritto internazionale pubblico**".

- Principi applicabili al trattamento dei dati personali: **trasparenza**; **minimizzazione dei dati**; **responsabilità generale del responsabile del trattamento** (ex art. 5);

- **Onere** della prova di un'**informativa dettagliata** sul trattamento dei dati personali (ex art. 14), del relativo **consenso "esplicito"** (ex artt. 4, n. 8 e 7, co. 1) nonché della conformità del trattamento dei dati al regolamento (ex art. 22, co. 1) **a carico del responsabile del trattamento**;

- Procedure e meccanismi per l'esercizio dei diritti dell'interessato (art. 12)

Il responsabile del trattamento predispone altresì i mezzi per inoltrare le richieste **per via elettronica** qualora i **dati** siano **trattati con modalità automatizzate**

- Diritto di accesso dell'interessato (art. 15)

Se l'interessato presenta la **richiesta in forma elettronica**, le informazioni sono fornite in formato elettronico, salvo indicazione diversa dell'interessato

- Diritto all'oblio e alla cancellazione (art. 17)

Obbligo del responsabile del trattamento che abbia divulgato dati personali di informare i terzi della richiesta dell'interessato di **cancellare tutti i link verso tali dati, le loro copie o riproduzioni**

- Diritto alla portabilità dei dati (art. 18)

Diritto al trasferimento dei dati personali da un sistema di trattamento elettronico a un altro, senza che il responsabile del trattamento possa impedirlo.

Come presupposto e al fine di migliorare l'accesso dell'interessato ai dati personali che lo riguardano, è previsto il **diritto di ottenere tali dati dal responsabile del trattamento in un formato elettronico strutturato e di uso comune**.

- Responsabilità del responsabile del trattamento (art. 22)

Politiche e **misure adeguate** per garantire ed essere in grado di dimostrare che il trattamento dei dati personali effettuato è conforme al presente regolamento:

(a) la **conservazione** della documentazione ai sensi dell'articolo 28;

(b) l'attuazione dei requisiti di **sicurezza dei dati** di cui all'articolo 30;

(c) l'esecuzione della **valutazione d'impatto sulla protezione dei dati** ai sensi dell'articolo 33;

(d) il rispetto dei requisiti di **autorizzazione preventiva o di consultazione preventiva dell'autorità di controllo** ai sensi dell'articolo 34, paragrafi 1 e 2;

(e) la designazione di un **responsabile della protezione dei dati** ai sensi dell'articolo 35, paragrafo 1.

- Articolo 23 - Protezione **fin dalla progettazione** e protezione **di default**

  - Definizione dei sistemi informativi sanitari nel rispetto delle misure di sicurezza previste dalla normativa vigente.
  - In particolare, lo strumento informatico deve essere progettato in modo tale da contenere gli abusi di dati personali e sensibili dei pazienti, attraverso opportune limitazioni d'uso e trattamento

- Documentazione (art. 28)

Obbligo per i responsabili e gli incaricati del trattamento di **conservare la documentazione** delle operazioni effettuate sotto la propria responsabilità

Capo IV; Sezione 2 – Sicurezza dei dati

Oneri a carico del responsabile del trattamento:

- **Notificazione** di una violazione dei dati personali all'autorità di controllo (art. 31);
- **Comunicazione** di una violazione dei dati personali all'interessato (art. 32). Eccezione (art. 32, co. 3)

"**Non** è richiesta la comunicazione di una violazione dei dati personali all'interessato se il responsabile del trattamento dimostra in modo convincente all'autorità di controllo che ha utilizzato le **opportune misure tecnologiche di protezione** e che tali misure erano state **applicate ai dati violati**. **Tali misure tecnologiche di protezione devono rendere i dati incomprensibili a chiunque non sia autorizzato ad accedervi**"

- Valutazione d'impatto sulla protezione dei dati (art. 33); autorizzazione preventiva e consultazione preventiva (art. 34)

a) Obbligo per responsabili e incaricati del trattamento di effettuare una valutazione d'impatto in materia di protezione dei dati **prima** di trattamenti che presentino rischi al riguardo;

b) Controllo preliminare nei casi in cui il responsabile del trattamento o l'incaricato del trattamento devono ottenere l'autorizzazione preventiva dell'autorità di controllo o consultare tale autorità prima di trattare i dati

- Designazione del **responsabile della protezione dei dati** (art. 35)

Nuova figura obbligatoria per il settore pubblico e, nel settore privato, per le grandi imprese o quando le attività principali del responsabile del trattamento e dell'incaricato del trattamento consistono in trattamenti che richiedono il controllo regolare e sistematico degli interessati.

- Compiti del responsabile della protezione dei dati (art. 37)

a) **informare** e **consigliare** il responsabile del trattamento o l'incaricato del trattamento in merito agli obblighi derivanti dal presente regolamento e conservare la documentazione relativa a tale attività e alle risposte ricevute;

b) **sorvegliare** l'attuazione e l'applicazione delle politiche del responsabile del trattamento o dell'incaricato del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la formazione del personale che partecipa ai trattamenti e gli audit connessi;

c) **sorvegliare** l'attuazione e l'applicazione del presente regolamento, con particolare riguardo ai requisiti concernenti la protezione fin dalla progettazione, la protezione di default, la sicurezza dei dati, l'informazione dell'interessato e le richieste degli interessati di esercitare i diritti riconosciuti dal presente regolamento;

d) **garantire** la conservazione della documentazione di cui all'articolo 28;

e) controllare che le violazioni dei dati personali siano documentate, notificate e comunicate ai sensi degli articoli 31 e 32;

f) **controllare** che il responsabile del trattamento o l'incaricato del trattamento effettui la valutazione d'impatto sulla protezione dei dati e richieda l'autorizzazione preventiva o la consultazione preventiva nei casi previsti dagli articoli 33 e 34;

g) **controllare** che sia dato seguito alle richieste dell'autorità di controllo e, nell'ambito delle sue competenze, cooperare con l'autorità di controllo di propria iniziativa o su sua richiesta;

h) **fungere da punto di contatto** per l'autorità di controllo per questioni connesse al trattamento e, se del caso, consultare l'autorità di controllo di propria iniziativa.

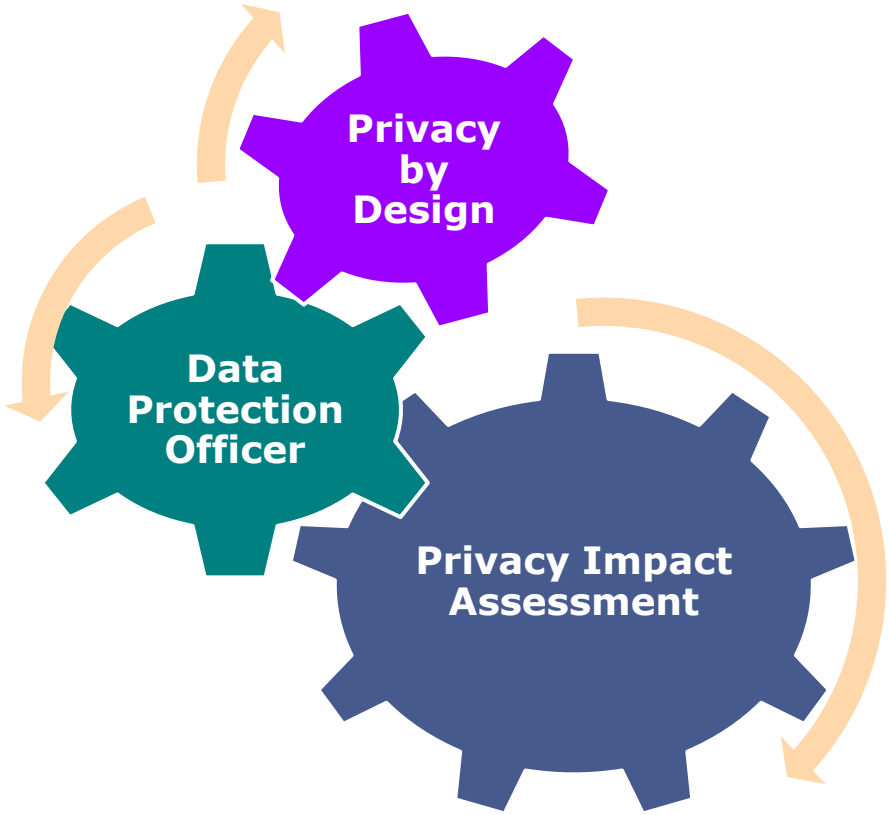
Parere del Garante su uno schema di decreto del Presidente del Consiglio dei ministri in materia di fascicolo sanitario elettronico - 22 maggio 2014

"5. Responsabile della protezione dei dati. Nel tavolo di lavoro si è fatto riferimento alla figura del "responsabile della protezione dei dati". Al riguardo, pur condividendo la scelta di non inserire nel regolamento una disposizione che obblighi i titolari del trattamento ad istituire tale figura, l'Autorità, in ragione della particolare delicatezza delle informazioni trattate nell'ambito dell'FSE utilizzate per le molteplici finalità previste dalla legge, auspica che ogni titolare coinvolto dall'applicazione del presente decreto individui al suo interno una figura di responsabile della protezione dei dati che interloquisca con il Garante, anche in relazione ai casi di data breach previsti nell'articolo 24, comma 9 dello schema".

Riflessioni finali

- Assoluta continuità rispetto alla direttiva 95/46/EC per ciò che concerne i principi generale (eccezioni: "minimizzazione utilizzo dati" e "Privacy by Design");
- Ambiti di effettiva innovazione:
  a) attenzione ai profili pratici della protezione dei dati personali (es. implementazione dei principi e applicazione dei diritti e degli obblighi);
  b) semplificazione e riduzione dei costi (es. eliminazione dell'obbligo generale di notificazione all'autorità di controllo prima di procedere al trattamento ed introduzione dell'obbligo di notificare eventuali violazioni)

- Strutture sanitarie quali titolari del trattamento dei dati ad alta complessità. Per questo occorrono **nuove policy organizzative**



Grazie per l’attenzione

Maria Gabriella Virone

C.I.R.S.F.I.D. – Alma Mater Studiorum Università di Bologna

mariagabriella.virone@gmail.com