Tecnologia e Management delle Aziende sanitarie, l'approccio organizzato alle misure del Regolamento 2016/679 UE

FILOMENA POLITO -24 GIUGNO 2016

SPID ed Identità Digitale: Mercificazione, risorsa, opportunità o pericolo?

Associazione Nazionale
Privacy Information Healthcare Manager

Libera associazione di esperti e cultori della materia per promuovere, all'interno del sistema sanitario, l'utilizzo corretto delle informazioni e il rispetto dei diritti dell'utenza

- **Aziende Sanitarie**
- **Consorzi di aziende sanitarie**
- **Medici**
- **Informatici**
- **Ingegneri**
- **Data Protection Officer**
- **Giuristi**

..i dati SONO PREZIOSI

..i dati devono essere protetti…

… svolgiamo un attività molto pericolosa

E ancora c'è chi associa PRIVACY a burocrazia

..o pensa che il suo rispetto si traduca solo in una serie di formalismi…..

European Commission

Data Protection

Regolamento UE 2016/679

in vigore dal 24 maggio 2016

Cambiano i termini….ma soprattutto cambia l'obiettivo

Da **FORMA** a

SOSTANZA

Da regole solo formali
a un sistema interno ma tracciabile di governo dei dati

Non abbiamo tempo da perdere…

Regolamento UE Privacy: Eccolo!

4 Maggio 2016

Pubblicazione in Gazzetta Ufficiale Europea

24 Maggio 2016

Entrata in vigore

25 Maggio 2018

Piena applicazione

Adeguarsi da subito, non aspettare!

Solo 699 giorni !!!!

L'Azienda Sanitaria deve garantire

adeguata sicurezza dei dati personali

protezione, mediante misure tecniche e organizzative adeguate da trattamenti non autorizzati o illeciti, perdita, distruzione o danno accidentali

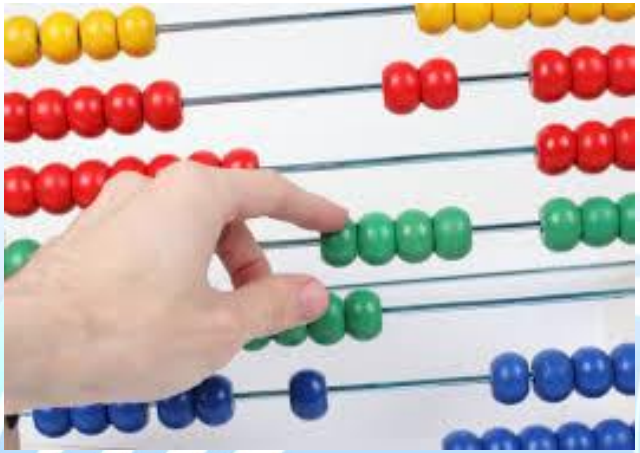
SISTEMA GESTIONALE PRIVACY

ACCOUNTABILITY

i dati sono trattati sotto la responsabilità dell'Azienda, che **assicura** e **documenta** che il trattamento sia conforme al Regolamento

Principio di **RENDICONTAZIONE**

Obbligo di **RENDERE CONTO**



comprovare

L’Azienda sanitaria
deve comprovare il rispetto di tali misure

Attuazione di
MISURE e PROCEDURE

CONSERVAZIONE PROVE

L'Azienda deve **riesaminare e aggiornare** le misure tecniche e organizzative attivate

RENDERSI CONTO PER RENDERE CONTO

Valutare
Decidere
Fare
Controllare
Dimostrare

L'Azienda **prima di attivare**
un trattamento di dati mette in atto
misure tecnico- organizzative adeguate

Funzione di compliance

Privacy by design

PRIVACY BY DESIGN E PRIVACY BY DEFAULT

- **Art. 23**

Al momento di determinare i mezzi del trattamento e all'atto del trattamento stesso, il responsabile del trattamento, **tenuto conto dell'evoluzione tecnica e dei costi di attuazione, mette in atto adeguate misure e procedure tecniche e organizzative in modo tale che il trattamento sia conforme** al presente regolamento e **assicuri la tutela dei diritti dell'interessato**

VALUTAZIONE D'IMPATTO PRIVACY

periodica attività di controllo interno

verifica adeguatezza misure di sicurezza organizzative e tecniche e rispondenza a disposizioni vigenti

SISTEMA DOCUMENTALE PRIVACY

Registro dei trattamenti

L'Azienda deve designare un Data Protection Officer

Una funzione chiave per l'innovazione….. molto delicata

Il DPO è designato sulla base:

-delle qualità professionali
-della conoscenza specialistica della normativa
-della conoscenza specialistica delle specifiche prassi in materia di protezione dei dati
-della capacità di assolvere ai compiti a questo delegati dalla legge

«competenza»

Il Direttore Generale sostiene il DPO nell'esecuzione dei compiti assegnati:

- fornendogli le risorse necessarie per assolverli, accedere ai dati personali e ai trattamenti
- mantenere la propria conoscenza specialistica.

Gli Interessati possono contattare il DPO per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei diritti.

DPO
DATA PROTECTION OFFICER

Il DPO deve:

Informare e fornire consulenza alla Direzione, ai Responsabili e agli Incaricati in merito agli obblighi di legge

DATA PROTECTION OFFICER

Sorveglia l'osservanza della legge e delle policy aziendali compreso:

-l'attribuzione delle responsabilità

-la formazione del personale che partecipa ai trattamenti e ai controlli

Fornisce parere in merito alla VIP e ne sorveglia lo svolgimento

DP
DATA PROTECTION OFFICER

Coopera con il Garante

DATA PROTECTION OFFICER

DPO
DATA PROTECTION OFFICER

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

referente con il Garante anche in relazione ai casi di data breach

Nel SSN il DPO è già previsto :
- nelle Linee Guida sul DSE
-nel DPCM sul FSE

Dati e identità

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Ruolo essenziale del Garante

Il Garante continua a segnalare cosa non va nel sistema digitale…

Parere su uno schema di D.L.gs recante Modifiche ed integrazioni al CAD - 9 giugno 2016

- necessità di garantire effettiva e piena coerenza del quadro normativo con altri strumenti in itinere o appena adottati (il regolamento eIDAS e i decreti su SPID, trasparenza ed anticorruzione)… è essenziale che sia assicurata chiarezza nelle definizioni dei processi e delle responsabilità,

lo schema prevede un "ufficio dirigenziale generale …» di difficile collocazione presso le strutture delle amministrazioni di piccole dimensioni.

Si nota il mancato coordinamento, di tale responsabile o (che svolge anche funzioni di "difensore civico digitale") con il DPO

Il Garante ….invita il Ministero, visto che il Regolamento europeo (UE) 2016/679 sancisce l'obbligatorietà della designazione di DPO nelle PP.AA., a esaminare l'opportunità che il suddetto responsabile coincida con il DPO

E chiarisce come è necessario approcciarsi con visione organizzativa alle misure di legge

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Parere alla Regione Lazio sullo "Schema tipo di Regolamento aziendale sul trattamento dei dati nei processi di diagnosi e cura" – 12 maggio 2016

UMBERTO I
POLICLINICO DI ROMA

APiHM
Privacy and Information Healthcare Manager Association

UMBERTO I
POLICLINICO DI ROMA

il Policlinico ha censito i trattamenti di dati di pertinenza, indicandone i dati personali a ciò indispensabili e i presupposti di liceità e le finalità istituzionali perseguite

Individuato:

- le responsabilità nel trattamento dei dati
- Le indicazioni operative e di vigilanza dell'operato dei soggetti designati

UMBERTO I
POLICLINICO DI ROMA

Le modalità organizzative attraverso cui dare attuazione agli adempimenti di protezione dei dati personali tenendo conto di:

- dimensione,
- organigramma e
- tipologia dei processi di diagnosi e cura della struttura sanitaria

UMBERTO I
POLICLINICO DI ROMA

- censimento degli strumenti informatici con i quali sono trattati i dati personali dei pazienti, evidenziando rischi e responsabilità.

Dati e identità

Ben 3 pareri sullo SPID

E per l'applicazione dello SPID nel sistema Sanitario quali dubbi nascono????

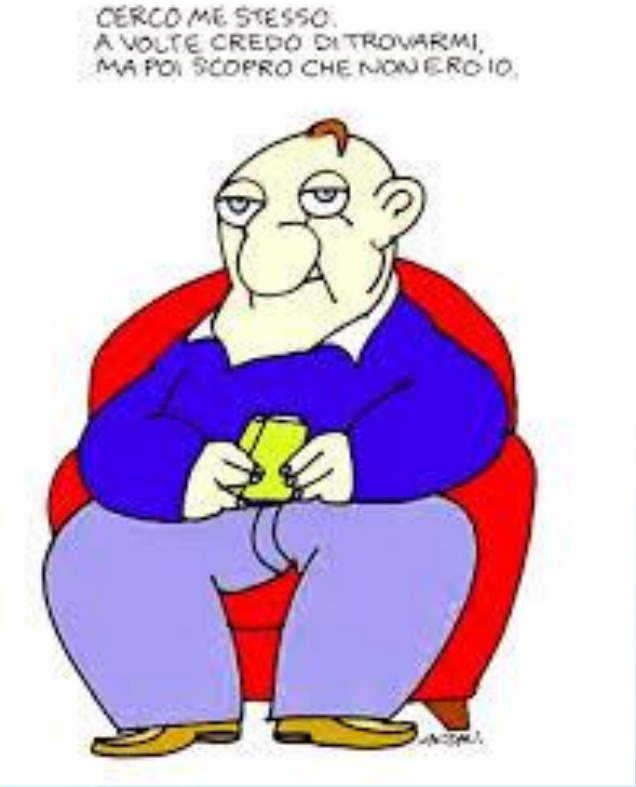
SPID
Sistema Pubblico
di Identità Digitale

Servizi on line erogati dal SSN

- Distribuzione referti
- Prenotazione prestazioni
- Pagamento delle prestazioni erogate
- Fascicolo Sanitario Elettronico
- Gestione istanze di accesso
- Sistemi di valutazione della qualità del servizio erogato

I dati personali trattati nel sistema Sanitario hanno anche valore medico legale…

In taluni casi la legge ha previsto una anticipazione della capacità di agire per i minorenni cui eroghiamo particolari prestazioni….



Trattiamo anche dati c.d.» a maggior tutela»…

Trattiamo spesso dati di cittadini stranieri….

Valutazione di Impatto privacy

- Da attivare ogni volta che l'azienda sanitaria deve consentire l'utilizzo dello SPID per l'erogazione del servizio digitale

È necessario attivare nuove misure e adottare un modello di organizzazione

presidente@apihm.it

filomenapolito.dpo@gmail.com

Grazie