ACCREDITED FOR ORGANIZATION BY
JOINT COMMISSION INTERNATIONAL

Servizio Sanitario Regionale
AZIENDA OSPEDALIERO – UNIVERSITARIA
"OSPEDALI RIUNITI" DI TRIESTE
Ospedale di rilievo nazionale e di alta specializzazione
(D.P.C.M. 8 aprile 1993)

HEALTH PROMOTING HOSPITAL
Ospedali per la Promozione della Salute
HPH *Una rete dell'OMS*

e-Health e ICT security stato dell'arte e criticità

dove stiamo andando e che cosa è già cambiato nel nostro modo di gestire i dati

Graziano de' Petris
graziano.depetris@aots.sanita.fvg.it

Responsabile Ufficio Privacy e Gestione dati sensibili
Coordinatore Gruppo Privacy e Sicurezza Sanità Regione Friuli Venezia Giulia

Internet *ha cambiato*
il nostro modo di ***comunicare***
il nostro modo di ***relazionarci***
il nostro modo di ***vedere il mondo***

e quindi

il nostro modo di ***lavorare***

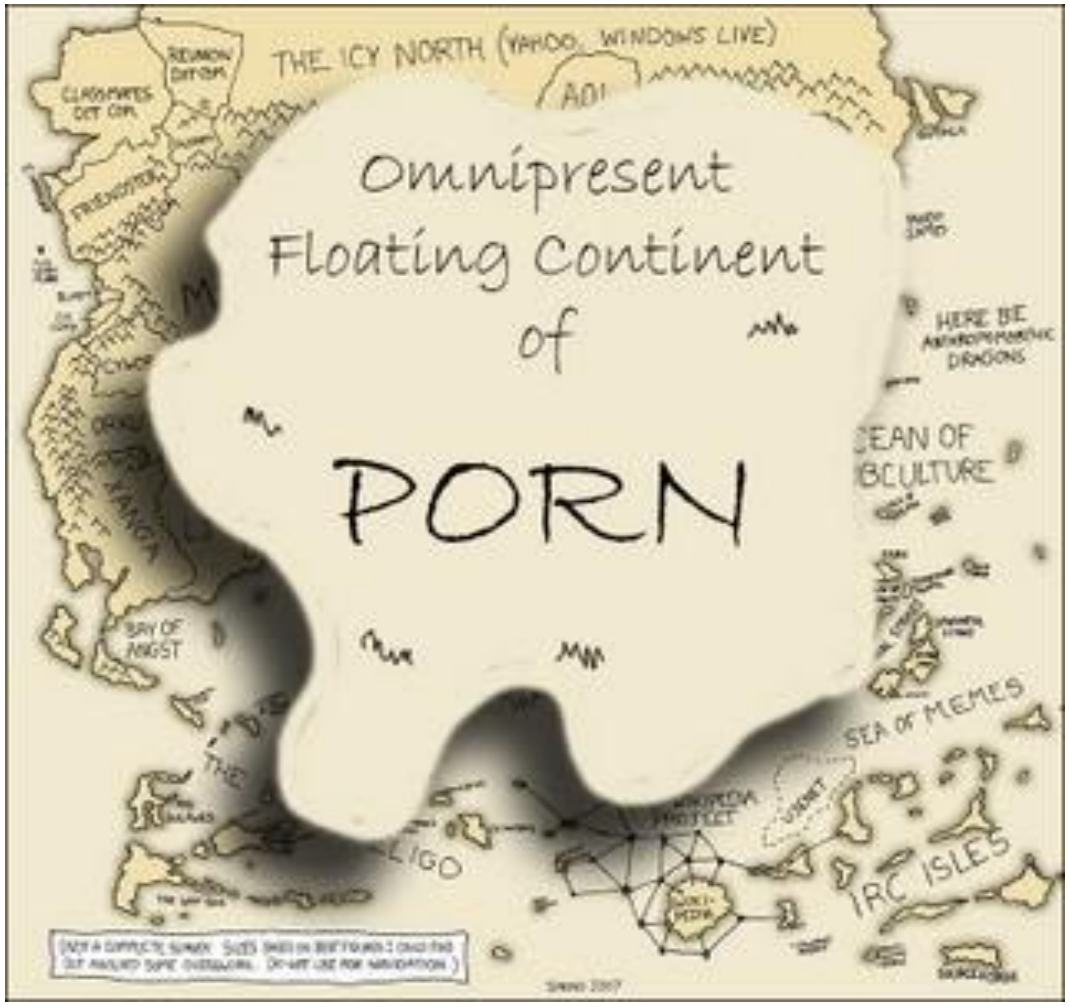

You are here
Map of the Internet, The Opte Project, www.opte.org

C'è stato un cambiamento epocale…

ora viviamo nella
Società della Conoscenza

di cui Internet è il Pilastro

The Conversation
The Art of Listening, Learning, and Sharing
Brought to you by
Brian Solis and JESS3
Social Bookmarks
Comment & Reputation
Crowdsourced Content
Blog Platforms
Blogs/Conversations
Blog Communities
Micromedia
Lifestreams
Specific to Twitter
SMS/Voice
Social Networks
Niche Networks
Customers Service Networks
Location
Video
Video Aggregation
Documents
Events
Music
Wiki
LiveCasting - Video and Audio
Pictures



15% *dei siti Web*

3,5 miliardi *di dollari di fatturato*

300 *nuovi siti porno creati ogni giorno* *(fonte Family Safe Media)*

Google maps Italia

via portuense 1645 roma

Cerca sulle mappe

Site Search Ricerca sul web

Via Portuense, 1645

00054 Fiumicino RM

Indicazioni stradali Cerca nelle vicinanze Altro ▾

Attività commerciali selezionati presso questo indirizzo:

Green Utility S.P.A. -

Marziali Costruzioni Generali Societa A Responsabilita Limitata -

Volare Shuttle Societa' Consortile A R.L -

Tutte le attività commerciali presso questo indirizzo »

L'evoluzione tecnologica
ha portato ad un cambiamento
nel modo di comunicare

ora tutelare la riservatezza
non è più così facile….

Con il cosiddetto Web 2.0 e 3.0

Sono cambiate le regole del gioco

Facebook, social network, blog,…

nel Web database, nel Web semantico

i siti *li fanno gli utenti!*

e cliccando sui link,

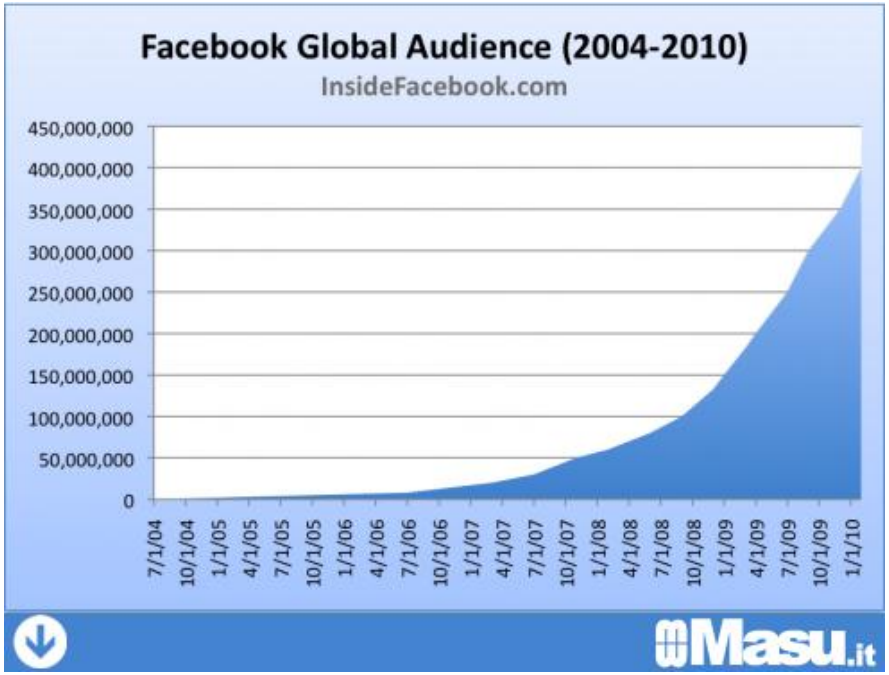
installiamo sui nostri PC

quello che vogliono loro

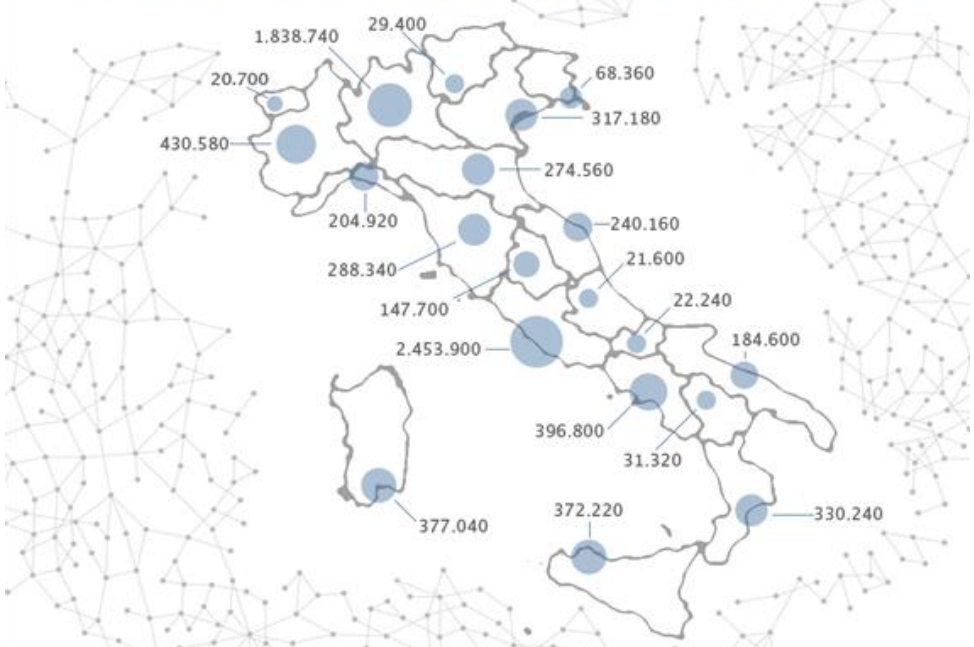
gli stessi PC da cui si accede ai dati clinici?

Facebook

quel luogo *virtuale* fatto di *informazioni reali*
dove tutti si fanno gli affari degli altri
ha superato i 450.000.000 di utenti
18 milioni in Italia



facebook in Italia

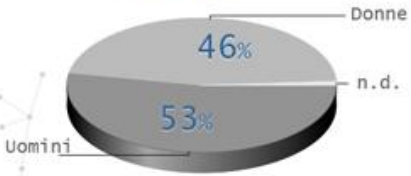


18MM registrati

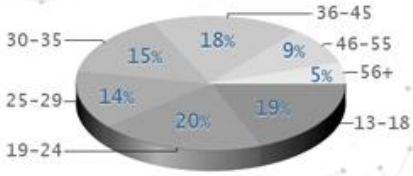
12MM al giorno

4MM da mobile

Sesso



Età



gennaio 2011

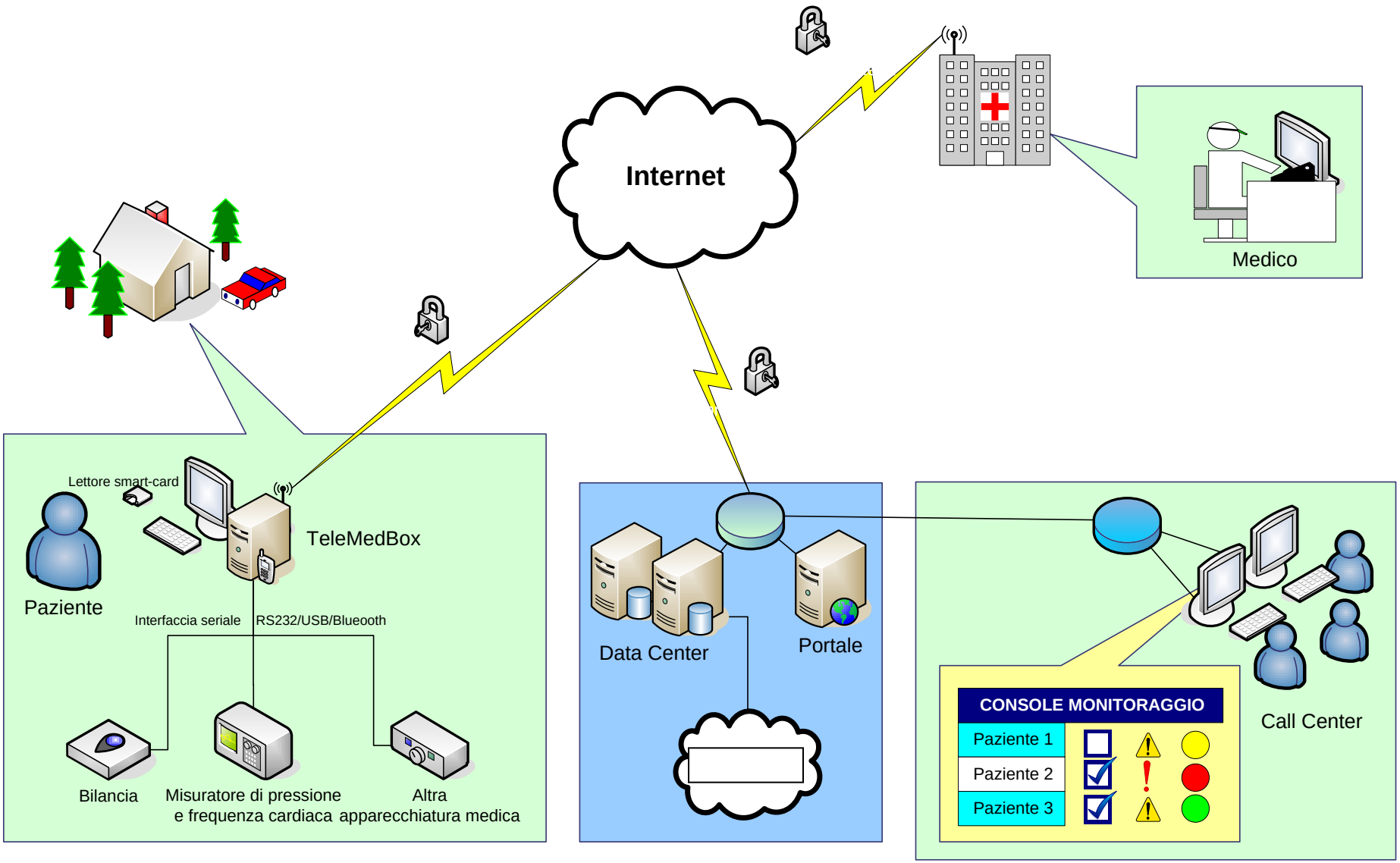
source: www.facebook.com/ads

Ma i dati *non sono* nel computer…

…se il PC è in rete
i dati sono in rete!

…e oramai i PC sono sempre in rete…

...gli stessi PC
con i quali si fa telemedicina?



E *come* conserviamo i dati importanti?

- 3 persone su 5 hanno *perso dati riservati* per il guasto di un PC
- Il 10% dei notebook viene *perso o rubato* ogni anno
- Il 70% di tutti i dati sono *copiati anche sugli endpoint* (notebook, smartphone, dischi o chiavette USB,….)
- 1 dispositivo USB su 2 contiene *dati sensibili*

Come possiamo proteggere i nostri dati?

La sicurezza informatica non è un'invenzione né del Garante per la protezione dei dati personali, né dell'Autorità per l'informatica nella P.A.,

né del Ministro Brunetta…

E' soltanto una *logica comportamentale*

applicata ad uno *strumento di comunicazione*

(il vecchio PC…)

Un comportamento anomalo in rete *non è facilmente identificabile!*

Che cosa si deve intendere per “Security ICT” in Sanità?

lo *studio*, lo *sviluppo*, la *messa in pratica*

e la **verifica continua**

delle strategie, delle politiche e dei piani operativi

atti a prevenire, fronteggiare e superare

eventi di natura dolosa e/o colposa

che possono *danneggiare*, *modificare*, *cancellare*

ma anche *diffondere* a soggetti non autorizzati

le informazioni cliniche degli utenti

necessarie per una corretta scelta

diagnostica e terapeutica

… cioè per la tutela dei dati
e delle informazioni personali
che vengono affidati al medico
dagli utenti

…quindi anche da noi tutti!

alcune semplici considerazioni

- il furto di un dato *non lascia alcuna traccia apparente sull'originale*
- un utilizzo inopportuno, inconsapevole o *incosciente* delle risorse informatiche può provocare danni gravissimi all'intero patrimonio informativo
- Proteggere i dati è molto difficile perché l'accessibilità è possibile *da innumerevoli punti*

Il pericolo maggiore

La bassa percezione di reato

La Sicurezza dell'Informazione

Dal 1993 esiste il ***reato telematico***

(informatico o a mezzo informatico)

Caratteristiche:

- alta potenzialità offensiva

- rapida scomparsa degli elementi probatori

La Sicurezza dell'Informazione

Per contrastare efficacemente il
reato telematico è indispensabile:

- Il rispetto di regole semplici ma rigorose
- La collaborazione di tutti
- La massima tempestività d'intervento

Quali regole, quindi?

- Regole forti per la protezione della *Privacy*
- Regole forti per la protezione *forte* dei dati “sensibili”
- Regole *applicabili* per il trattamento dei dati in sicurezza

La Sicurezza dell'Informazione
come si ottiene

- **Regolamenti** semplici e praticabili

  Non condividere ciò che non è indispensabile condividere

- **Protocolli operativi** ben definiti, derivati dall'applicazione delle Norme

Sicurezza = Consapevolezza

Consapevolezza = Procedure

La Sicurezza dell'Informazione
come si può ottenere?

- Principalmente con la Formazione

di

tutti gli addetti ai lavori

Quali misure applicare?

- Policy IT di sicurezza
- Regolamenti
- Distribuzione di responsabilità (corretta e *legalmente sostenibile*)
- Piano per il Disaster Recovery
- Piano di formazione
- Attuare controlli periodici preventivi (dei quali tutti siano *consapevoli*)

La Sicurezza dell'Infrastruttura: *elementi di base*

- Accesso ai PC in modalità USER
- Accessi amministrativi con password personale *forte (Amministratori di sistema…)*
- Cambio periodico di tutte le password
- Aggiornamenti di sicurezza
- Log, log, log, (nel rispetto della legge)

La Sicurezza dell'Informazione: *in conclusione*

Si ottiene

principalmente

attraverso l'applicazione

di *procedure*

e di *modalità operative*

ben definite

La Sicurezza del dato clinico
come la gestiamo in pratica?

Leggi e Normative
ci sono!

- La L 547/93 ha introdotto la normativa sui *crimini informatici* introducendo nel Codice Penale nuove fattispecie di reato:

- Accesso abusivo a sistemi informatici
- Detenzione e diffusione abusiva di pwd
- Diffusione di malware

Leggi e Normative *ci vengono in aiuto*

- Art. 615 ter "accesso abusivo ad un sistema informatico o telematico“
- Art. 615 quater "detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici“
- Art. 615 quinquies "diffusione di programmi diretti a danneggiare o interrompere un sistema informatico“

Leggi e Normative
ci vengono in aiuto

- Art. 616 violazione della corrispondenza "anche per via telematica“
- Art. 617 quater "intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche“
- Art. 640 ter "frode informatica“

Leggi e Normative
ci vengono in aiuto

Accesso Abusivo ad un sistema informatico o telematico (Art.615 CP)

  - Abusiva introduzione in un sistema informatico o telematico protetto da misure di sicurezza
  - Permanenza contro la volontà espressa o tacita di chi ha il diritto di escluderlo
- Sanzione: reclusione sino a tre anni
- Procedibilità: a querela di parte

Leggi e Normative
ci vengono in aiuto

Ipotesi aggravata - 615terCp

- Se commesso da PU o incaricato Pubblico Servizio
- Se commesso da operatore di sistema
- Se ne deriva distruzione o danneggiamento del sistema o interruzione totale o parziale del suo funzionamento o distruzione o danneggiamento dei dati, di informazioni, di programmi contenuti

- Sanzione : reclusione da uno a cinque anni
- Procedibilità: d'ufficio

Leggi e Normative
ci vengono in aiuto

Ipotesi aggravata - 615terCp

- Sistemi informatici o telematici d'interesse militare o relative all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile

- Sanzione: reclusione da uno a cinque anni
- Procedibilità: d'ufficio

e anche

- Codice dell’Amministrazione digitale
- Codice di comportamento del Pubblico dipendente
- Codici deontologici specifici delle professioni sanitarie (da incrociare col codice Privacy…)

Ma allora non manca nulla!
Come procediamo?

Con la formazione

su *Sicurezza Informatica* e *Privacy*

e con il rispetto delle normative

sono obbligatori per Legge!

Prevenire è meglio che curare…

Quali strumenti adottare?

i Regolamenti

- sull'utilizzo delle risorse informatiche
- sull'erogazione e dismissione dei permessi d'accesso
- sulle modalità di effettuazione dei controlli

sono indispensabili!

Quali altri strumenti adottare?

la distribuzione delle responsabilità

- con mansionari precisi

- con nomine firmate *per presa visione*

è indispensabile!

Quali altri strumenti adottare?

la corretta configurazione in sicurezza
dei sistemi informatici
e delle reti

è obbligatoria per Legge!

Codice in materia di protezione dei dati personali

Il Codice definisce in maniera chiara gli elementi indispensabili per garantire la protezione dei dati e la fiducia degli utenti

- Riservatezza (Confidenzialità)
  - la protezione delle informazioni mediante l'accesso consentito soltanto agli autorizzati, la protezione delle trasmissioni, il controllo degli accessi, ...
- Integrità
  - la salvaguardia della correttezza dei dati, la difesa dalle manomissioni e da modifiche non autorizzate, il monitoraggio automatico degli accessi, …
- Disponibilità
  - la garanzia per gli utenti di poter disporre dei dati, delle informazioni e dei servizi, evitando la loro perdita o riduzione

Codice in materia di protezione dei dati personali

Art. 31: Obblighi di sicurezza

- I dati personali oggetto di trattamento devono essere custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee misure di sicurezza preventive, i rischi di:
  - distruzione o perdita, anche accidentale
  - accesso non autorizzato
  - trattamento non consentito
  - trattamento non conforme alle finalità della raccolta

Codice in materia di protezione dei dati personali le misure minime di sicurezza

- Art.4, comma 3, lettera a
  - il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31.

Codice in materia di protezione dei dati personali
le misure minime

- il controllo dell'accesso ai dati dev'essere garantito da
  - autenticazione informatica
  - credenziali di autenticazione
  - sistema di autorizzazioni

- Altre misure
  - adozione di procedure per la generazione e la custodia di copie di sicurezza dei dati
  - ripristino della disponibilità dei dati e dei sistemi
  - protezione dei dati sensibili o giudiziari contro l'accesso abusivo
  - aggiornamento periodico dei programmi per elaboratore volti a prevenire la vulnerabilità degli strumenti elettronici e alla correzione dei difetti del software

Codice in materia di protezione dei dati personali
trattamenti soggetti a rischi specifici

- Art.17:
  - Anche i dati diversi da quelli sensibili e giudiziari possono presentare particolari rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato
  - i rischi sono correlati alla natura dei dati o alle modalità o agli effetti del trattamento
  - i dati possono essere trattati nel rispetto di misure ed accorgimenti a garanzia dell'interessato, ove prescritti dal Garante in applicazione dei principi sanciti dal Codice e a seguito di una verifica preliminare all'inizio del trattamento

Codice in materia di protezione dei dati personali
il DPS

- Art.34, comma 1, lettera g): "tenuta di un aggiornato Documento Programmatico sulla Sicurezza"
  - richiede obbligatoriamente l'Analisi dei rischi che incombono sui dati sensibili o giudiziari e la descrizione delle contromisure adottate

il D.Lgs. 196/03
e l'Informatica Medica

Il Titolare dei trattamenti
è Civilmente e Penalmente
responsabile
per qualunque cosa accada
ai dati relativi alla salute

il D.Lgs. 196/03 e l'Informatica Medica *la sfida*

- E' difficile proteggere i dati sanitari garantendone la facilità d'accesso
- Il personale medico e infermieristico ha la reale necessità di trattare i dati al fine di curare i pazienti

- Disciplinare tecnico in materia di misure minime e adeguate di sicurezza (artt. da 33 a 36 del Codice)

- Provvedimento “Amministratori di Sistema” del 27/11/08 (entrato in vigore - *finalmente* - il15 dicembre 2009)

- Linee guida in tema di Fascicolo Sanitario Elettronico e dossier sanitario del 5 marzo 2009

- Regole tecniche in materia di generazione, apposizione e verifica delle firme digitali e di validazione temporale dei documenti informatici del 30 marzo 2009

Il Paradosso apparente

- la reale necessità del personale sanitario di ottenere facilmente le autorizzazioni di accesso ai dati e di accedervi

  e *contemporaneamente*

- l'obbligo di applicare le severe regole imposte, senza appesantire troppo l'organizzazione del lavoro

Con quali strumenti si può affrontare la sfida

- L'utilizzo delle attrezzature informatiche nel rispetto delle leggi *secondo logica e buon senso*
- La *distribuzione delle responsabilità*
- La *corretta configurazione* tecnica dei sistemi e dei permessi d'accesso
- L'*identificazione certa* degli utilizzatori dei sistemi informatizzati

I nuovi problemi

- I dispositivi medici *in rete*
- I dispositivi medici *che inviano dati all'estero*
- I dati sensibili *nel cloud*

La soluzione?

Serve *Professionalità*

UNIVERSITÀ
DEGLI STUDI DI TRIESTE

Dipartimento di Ingegneria Industriale e dell'Informazione

Master di II livello

Gestione della Privacy e della Sicurezza Informatica nella Pubblica Amministrazione

Anno accademico 2012/13

graziano.depetris@aots.sanita.fvg.it

depetris@ssic.units.it