Società Italiana
Telemedicina @ Sanità Elettronica

Convegno di studio su Privacy e Telemedicina

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

ORDINE AVVOCATI DI ROMA

App mediche: gadget elettronici o dispositivi medici? Criticità in tema di sicurezza e privacy

ing. Francesco Vellucci - CISSP

Comitato Consulenza SIT

Roma, 21 ottobre 2014

Sala Conferenze di Piazza Monte Citorio, 123/a

Il mercato

- **Più di 500 milioni di Utenti di App mediche entro il 2015.**
- **6.9 miliardi di dollari il business stimato del 2018**

fonte: min salute

Quindi → c'è sia mercato che interesse economico

L'Italia tra i principali consumatori di telefonini/ smartphones

→ Più di 17mila le App mediche già sul mercato italiano

Il mercato

Vantaggi potenziali delle App:

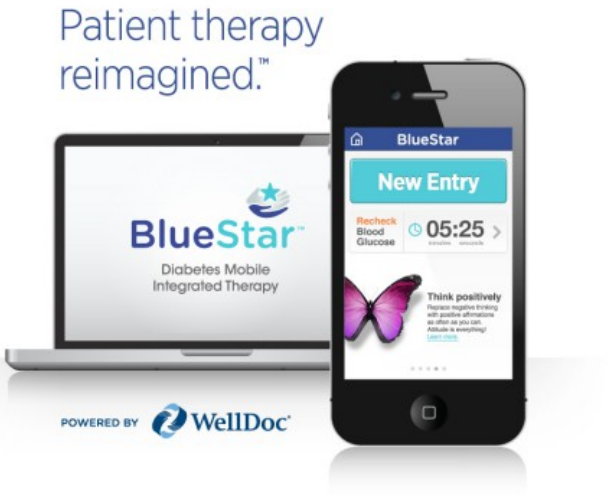
- facilitare diagnosi, terapia e formazione: → se in processo clinicamente controllato;
- ottimizzare i processi di cura: → Telemedicina;
- innescare un processo di «autogestione» e consapevolezza del paziente: → self management of health and disease in H2020

Il mercato

MobiUS SP1

AirStrip
Patient Monitoring

AUDIOMETRO PORTATILE (Inventis)



Dispositivi medici o Gadget?

Ovviamente…. Dipende……

«Dispositivi medici» solo se funzionalmente orientate alla diagnosi, cura, mitigazione, trattamento o prevenzione di una patologia

per FDA → da regolamentare solo se ha impatto diretto sulla diagnosi e sulla terapia: se è ad «alto rischio»

- **«alto rischio»**: App per pressione sanguigna, rilascio di insulina….
- **«basso rischio»:** App di informazioni sugli stili di vita, per monitoraggio terapie, per chiamate di emergenza….

Il gadget è un oggetto tendenzialmente inutile, ma che attira l'attenzione. In genere privo di pericolosità.

Quindi eventuali app mediche a bassa utilità e bassissimo rischio potrebbero rientrare nella categoria di gadget.

Ma è proprio così?

Mai sottovalutare un Gadget

- App = Programma SW in Ambiente operativo SW

- In quanto SW → potenziale presenza di Vulnerabilità sfruttabili da attaccanti malevoli

Mai sottovalutare una APP
(anche a basso rischio)

Valutare aspetti FUNZIONALI E di SICUREZZA: anche se una App è a basso impatto sulla Safety, può avere impatti sulla Security.

Valutare l'ambiente in cui la App è installata e le sue Protezioni

Valutare le protezioni dei canali di collegamento: es: Rete mobile, WiFi.

…non basta classificarle in base alle funzionalità e alla utilità clinica ma ne va definito il livello di rischio informatico

Safety, Privacy e Security integrate

Tra i principali 10 danni causati da dispositivi medici, App incluse:

- **Patient/data mismatches in EHRs and other health IT systems**
- **Interoperability failures with medical devices and health IT systems**
- **Caregiver distractions from smartphones and other mobile devices**

fonte: ECRI, USA (3/2013)

→ **Non considerati adeguatamente i potenziali rischi informatici di base, presenti in tutti i prodotti SW.**

→ **«consentire» le App ad Alto rischio solo in dispositivi mobili «embedded» certificati globalmente**

Data Breach

- **Tasso di crescita allarmante.**
- **Nel 2013 violati più di 7 milioni di records di Pazienti.**

  → *Caso CHSPSC nel 2014: "Esfiltrati" 4,5 milioni di records.*

- **Nel 2013 , 1,84 milioni gli adulti americani sono state vittime di furto di identità medica. In aumento del 20% rispetto all'anno precedente.**

- **Il costo annuale di tali violazioni si stima superi i 5.6 miliardi di $.**

fonte: Ponemon institute - 3/2014

Alcune azioni intraprese

- **2013: FDA → guida "Mobile Medical Applications"**
- **2014: EU → "mHealth «Libro Verde sulla sanità mobile**
- **2013: Min. Salute → avvio** regolamentazione delle App mediche e *Registro App Sanitarie*
- **2014: Garante → verifica di rispondenza di oltre 1200 App.**
- **2 ottobre 2014: FDA → lineaguida sulla Cybersecurity nei Medical Devices con raccomandazioni, non vincolanti, per i produttori**

Dai risultati del Garante, le Apps mediche:

- Richiesta di numero eccessivo di «consensi» all'accesso, spesso poco motivati.
- Nella metà dei casi assenza di corretta informativa Privacy, e/o rinvio a link esterni.
- Nel 15% dei casi le cose vanno bene , <u>almeno dal punto di vista della privacy</u>.

Quindi già le cose per la riservatezza dei dati personali non vanno molto bene

Dal punto di vista più ampio della Security è chiaro che non possono andare meglio

Riservatezza & Integrità dei Dati

Le App medicali, tendono ad essere percepite come «supporto al medico e alla propria salute».

Security through obscurity !

Rischio: Canale privilegiato per infiltrarsi negli smartphone personali

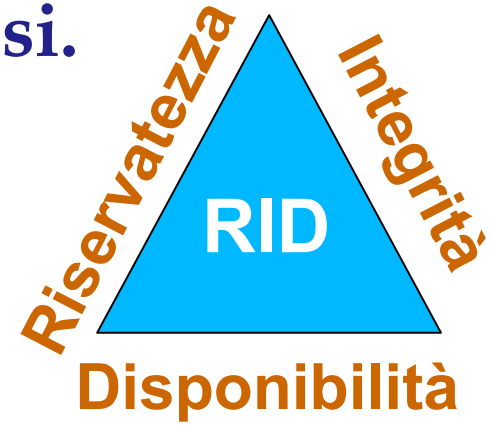
Oltre la Riservatezza dei dati:
Integrità e completezza della informazione

Proteggere tutti i lati del perimetro di sicurezza
→ Sistema Sanitario Connesso (connected health)

approccio olistico alla sicurezza

L'anello debole rischia di invalidare tutte le protezioni forti

- Controllo sicurezza della Apps;
- Controllo sicurezza ambiente in cui «girano» ;
- Controllo accessi.



BYOD

Bring Your Own Device

Rischi dall' "internet of Things"

Obiettivi dell'approccio olistico

- **Proteggere il Paziente**

- **Proteggere il Sistema Sanitario**

→ **Da gestione "contingente" a visione strategica e complessiva della protezione**

→ **Organizzare e governare le strategie di difesa**

Alcuni temi critici

Tecnici:

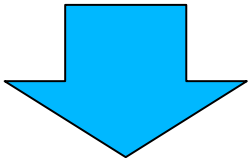
- Defence in depth-layered approach
- SSO integrato con gestione del contesto
- SIEM
- Bilanciare Funzionalità e Sicurezza

Amministrativi:

- Separation of duties;
- Least priviledge;
- No BYOD per App critiche
- Formazione Utente allaConsapevolezza:
  - **Passcode e auto lock per blocco dispositivo**
  - **Disabilitare bluetooth e WiFi se non usati**
  - **Non installare App da siti sconosciuti**
  - **Esaminare i permessi richiesti prima e dopo l'installazione**

Un MUST: la Consapevolezza

- **Sensibilizzazione sulla sicurezza per Pazienti, Medici, Operatori sanitari, Care givers**



  - **come identificare le informazioni riservate;**
  - **comprendere l'importanza della protezione dei dati e dei sistemi;**
  - **come scegliere e proteggere le password;**
  - **come utilizzare correttamente mail, social network e siti web;**
  - **come individuare tentativi di social engineering**

Due modelli

- Approccio «istituzionale»: registro di App, Certificazione
  - Pro: regole più generali e registro pubblico
  - Contro: Chi e in quanto tempo?
- Operare secondo lo schema della "trusted community e alle best practices.
  - Pro: Velocità
  - Contro: il «mercato» è sufficiente per fidarsi?

Entrambi hanno aspetti positivi, da contemperare e far necessariamente convivere

Una suggestione

- **Nel mondo e in Italia esistono numerosi siti di indicazioni sulle APP mediche**

- **Generalmente rispondono a fini commerciali**

Notizie, risorse e recensioni di Apps mediche e Accessori per iPad, iPhone e Android
mobimed
la medicina in tasca!

MedicApp
COLLECTION

iMedicalApps

Perché non pensare a una
Community di Esperti indipendenti
di Medicina, Privacy e Sicurezza
che promuova, attraverso un proprio sito, la CONSAPEVOLEZZA verso le App mediche?

Grazie per la pazienza