VIII Convegno Nazionale Fondazione AMD

AMD ASSOCIAZIONE MEDICI DIABETOLOGI
1974 ANNO DI FONDAZIONE

AMD FONDAZIONE onlus ASSOCIAZIONE MEDICI DIABETOLOGI

PALERMO, 17-19 NOVEMBRE 2016

Connettività e Telemedicina il problema della «Cybersecurity»

Lorenzo de Candia

- Telemedicina
- Medical Devices e connettività
- La Privacy: cosa dice il Garante
- La Password questa (s)conosciuta
- Comportamenti in Rete: il Pishing
- La Cybersecurity

TELEMEDICINA O TELEHEALTH

DEFINIZIONE DI TELEMEDICINA

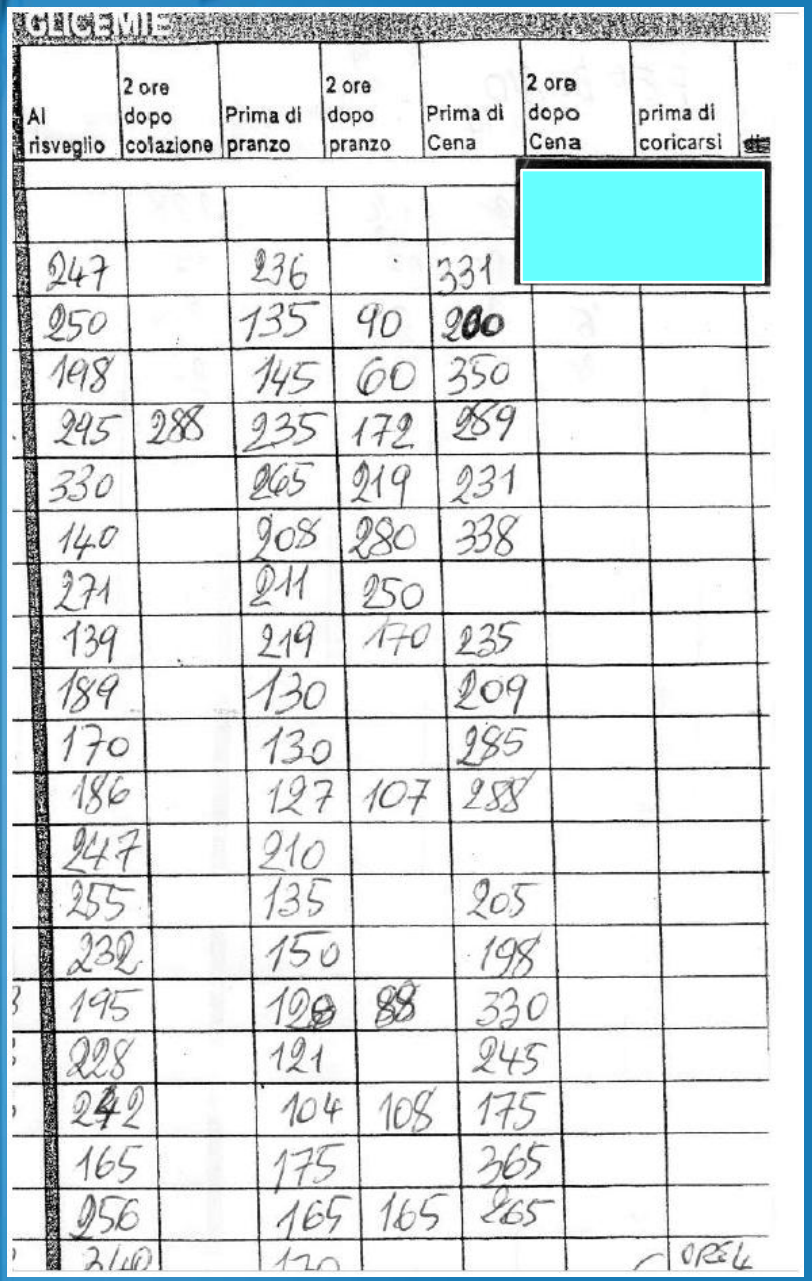
- Per Telemedicina si intende una modalità di erogazione di servizi di assistenza sanitaria, tramite il ricorso a tecnologie innovative, in particolare alle Information and Communication Technologies (ICT), in situazioni in cui il professionista della salute e il paziente (o due professionisti) **non si trovano nella stessa località**.
- La Telemedicina comporta la **trasmissione sicura** di informazioni e dati di carattere medico nella forma di testi, suoni, immagini o altre forme necessarie per la prevenzione, la diagnosi, il trattamento e il successivo controllo dei pazienti.

DEFINIZIONE DI TELEMEDICINA

- I servizi di Telemedicina **vanno assimilati a qualunque servizio sanitario diagnostico/ terapeutico**. Tuttavia la prestazione in Telemedicina non sostituisce la prestazione sanitaria tradizionale nel rapporto personale medico-paziente, ma la **integra** per potenzialmente migliorare efficacia, efficienza e appropriatezza.
- La Telemedicina deve altresì **ottemperare** a tutti i diritti e obblighi propri di qualsiasi atto sanitario.

DEFINIZIONE DI TELEMEDICINA

- Si precisa che **l'utilizzo di strumenti di Information and Communication Technology** per il trattamento di informazioni sanitarie o la condivisione on line di dati e/o informazioni sanitarie **non costituiscono** di per sé servizi di Telemedicina.
- A titolo esemplificativo non rientrano nella Telemedicina **portali di informazioni sanitarie, social network, forum, newsgroup, posta elettronica o altro**.



Al risveglio	2 ore dopo colazione	Prima di pranzo	2 ore dopo pranzo	Prima di Cena	2 ore dopo Cena	prima di coricarsi
247		236		331		
250		135	90	200		
198		145	60	350		
245	288	235	172	289		
330		265	219	231		
140		208	280	338		
271		211	250			
139		219	170	235		
189		130		209		
170		130		285		
186		127	107	288		
247		210				
255		135		205		
232		150		198		
195		120	88	330		
228		121		245		
242		104	108	175		
165		175		365		
256		165	165	265		

Questa NON è Telemedicina

TELEMEDICINA

CLASSIFICAZIONE		AMBITO	PAZIENTI		RELAZIONE
TELEMEDICINA SPECIALISTICA	TELE VISITA	sanitario	Può essere rivolta a patologie acute, croniche, a situazioni di post-acuzie	Presenza attiva del Paziente	B2C B2B2C
	TELE CONSULTO			Assenza del Paziente	B2B
	TELE COOPERAZIONE SANITARIA			Presenza del Paziente, *in tempo reale*	B2B2C
TELE SALUTE		sanitario	E' prevalentemente rivolta a patologie croniche	Presenza attiva del Paziente	B2C B2B2C
TELE ASSISTENZA		socio-assistenziale	Può essere rivolta ad anziani e fragili e diversamente abili		

* B2B: individua la relazione tra medici

B2B2C: individua la relazione tra un medico e un paziente mediata attraverso un operatore sanitario

B2C: individua la relazione tra medico e paziente

TELEMEDICINA SPECIALISTICA

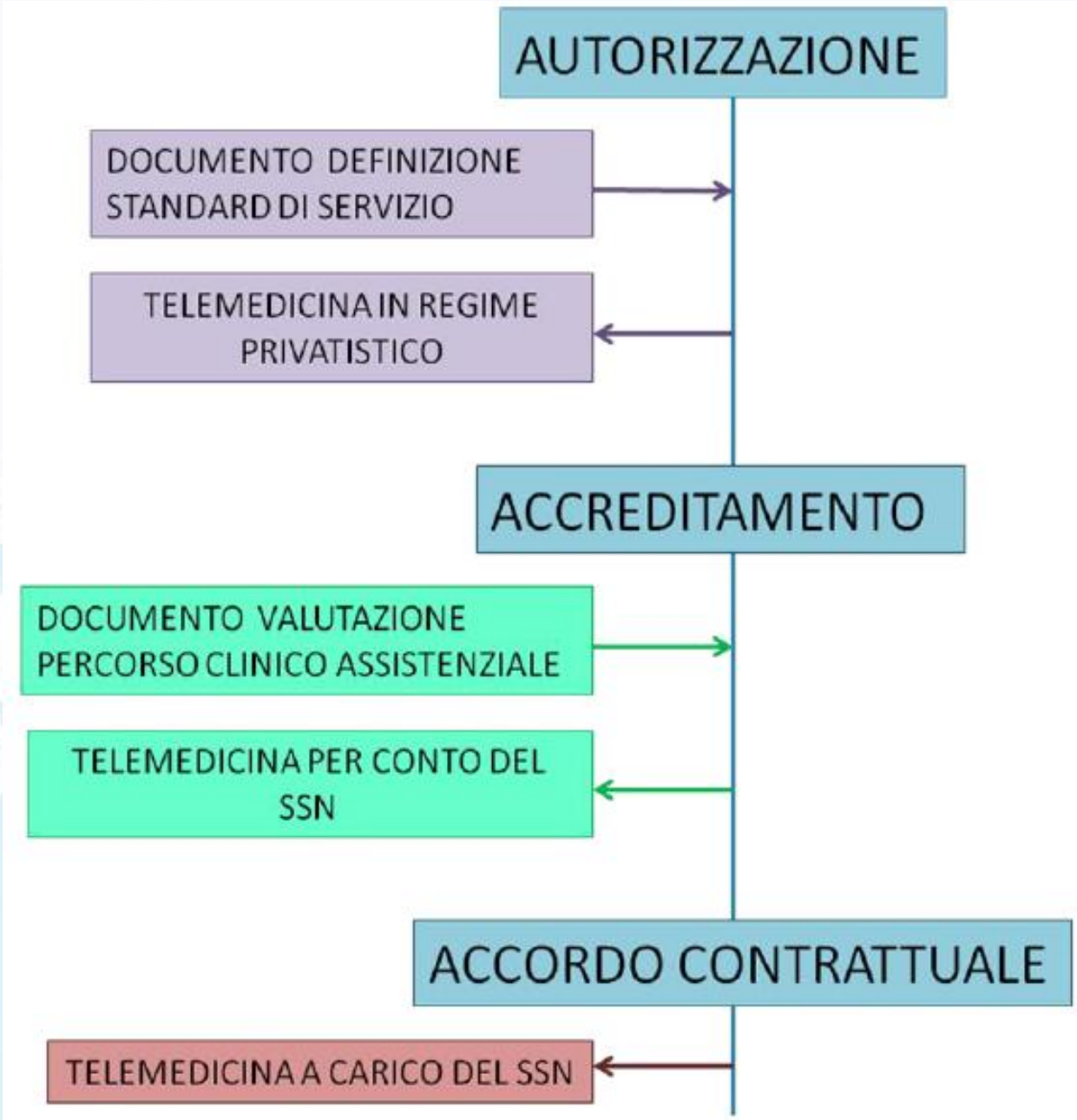
					FINALITA'				RELAZIONE*		
									B2C B2B2C	B2B2C	B2B
	PAZIENTI	AMBITO		Monitoraggio	Prevenzione	Diagnosi	Cura	Riabilitazione	Televisita	Telecooperazione sanitaria	Telecoonsulto
TELEMEDICINA DEI MEDICI SPECIALISTI	tutti	sanitario	TelePatologia (Laboratorio Biomedico e Anatomia Patologica)								
			TeleRadiologia								
			TeleCardiologia								
			TelePneumologia								
			TeleDermatologia								
			TeleOftalmologia								
			TelePsichiatria/TelePsicologia								
			TeleNeurologia								
			TeleChirurgia								
			TeleEmergenza								
			TeleRiabilitazione								
			TelePediatria								
			Telediabetologia	✦			✦		✦	✦	✦
TELEMEDICINA del TERRITORIO			TeleMMG								
			TelePLS								

* B2B: individua la relazione tra medici

B2B2C: individua la relazione tra un medico e un paziente mediata attraverso un operatore sanitario

B2C: individua la relazione tra medico e paziente

** tutte le specialità mediche e chirurgiche


AUTORIZZAZIONE
DOCUMENTO DEFINIZIONE STANDARD DI SERVIZIO
TELEMEDICINA IN REGIME PRIVATISTICO
ACCREDITAMENTO
DOCUMENTO VALUTAZIONE PERCORSO CLINICO ASSISTENZIALE
TELEMEDICINA PER CONTO DEL SSN
ACCORDO CONTRATTUALE
TELEMEDICINA A CARICO DEL SSN

- In **Svezia**, la Telemedicina è molto diffusa: nel 2008 era in uso in oltre 100 applicazioni e in oltre il 75% degli Ospedali. Le principali aree applicative sono la Televisita (paziente-medico), il telemonitoraggio e il teleconsulto radiologico.
- Anche la **Norvegia** ha investito sulle soluzioni di e-health, trovando ragione per la rilevanza della Telemedicina **nella bassa densità della popolazione a fronte delle grandi distanze per raggiungere l'Ospedale più vicino**. Molte sono le applicazioni in uso, tra cui: il Teleconsulto tra medico di medicina generale e specialista, la Tele-patologia, la Tele-radiologia, la Tele- psichiatria e servizi per il miglioramento della cura dei tumori.
- In **Gran Bretagna**, il Department of Health nel maggio 2008 ha finanziato un vasto programma di Teleassistenza e Telesalute, il Whole System Demonstrator (WSD) Programme, rivolto alle persone fragili e ai malati cronici, che ha coinvolto in 2 anni oltre 6000 pazienti e oltre 200 medici, probabilmente la più grande *sperimentazione* sistematica di Telemedicina mai condotta.

Telemedicine Kiosk

- Less than a decade ago, telemedicine was mainly used by hospitals and clinics for secure doctor-to-doctor consultations. But today, telemedicine has become a more common method for patients to receive routine care at home or wherever they are — often on their cellphones or personal computers.
- In the past several years, a growing number of employers have provided insurance coverage for telemedicine services enabling employees to connect with a doctor by phone using both voice and video. One limitation of such phone-based services is **physicians cannot always obtain basic vital signs such as blood pressure and heart rate**.
- That's where telemedicine kiosks offer an advantage. Hundreds of employers — often supported by their health insurers — now have them **installed in the workplaces**, according to consultants and two telemedicine companies that make kiosks, American Well and Computerized Screening, Inc.
- **Anthem** has installed 34 kiosks at 20 employers in the past 18 months. Kiosks are typically used for the same maladies that lead people to see a doctor **or seek urgent care** — colds, sore throats, upper respiratory problems, earaches and pink eye.
- Telemedicine doctors or nurse practitioners **can email prescriptions to clients' local pharmacies**. Employees often pay either nothing or **no more than $15 per session**, far less than they would pay with insurance at a doctor's office, an urgent care clinic or an emergency room.

Mercy Virtual by the Numbers

Critical Care
- 30 units
- 458 beds

Stroke
- 34 emergency departments

Hospitalist
- 3 facilities
- 193 beds

Sepsis
- 8 facilities
- 2,431 beds
- 13,271 patients served in 2014

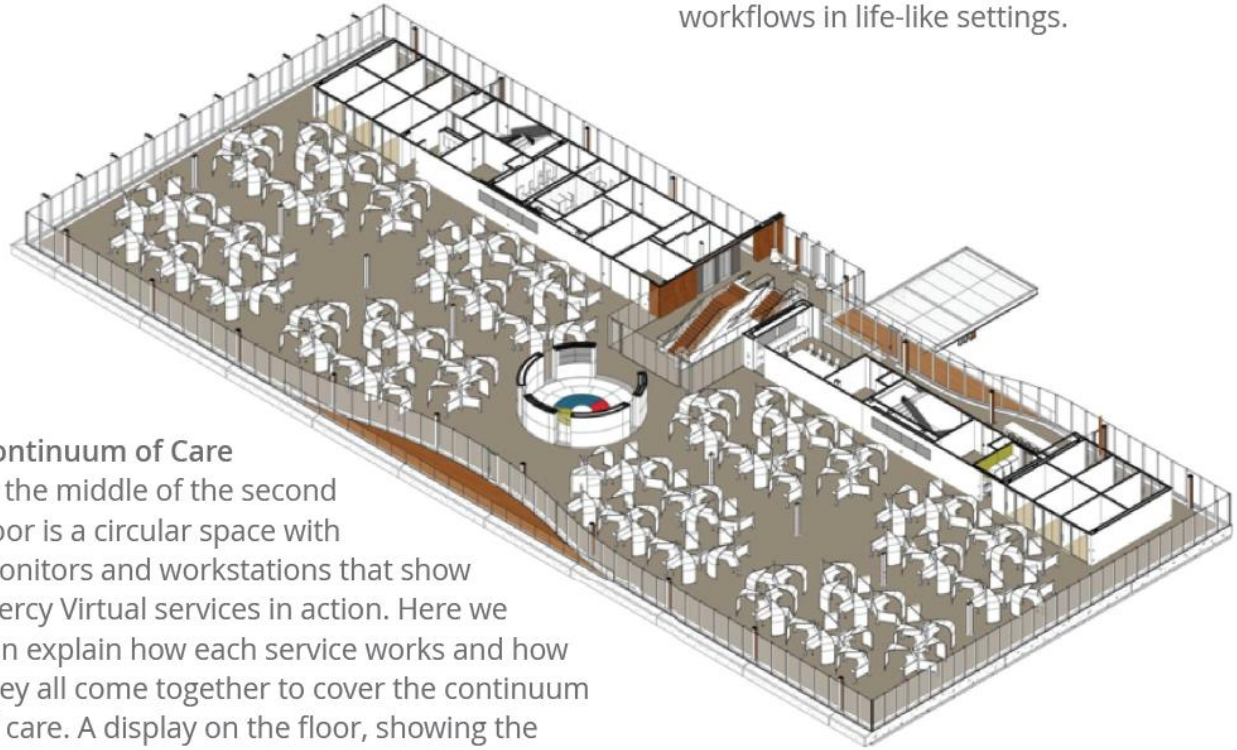
eConsults
- 31 physicians
- 32 patient sites

Managed Care
- 335,000 lives managed
- 285,000 Nurse On Call encounters annually

Co-workers
- 484 Mercy Virtual clinicians and support staff
- 330 located at new building

wearing the devices.

that will allow us to test technology and workflows in life-like settings.



Continuum of Care
In the middle of the second floor is a circular space with monitors and workstations that show Mercy Virtual services in action. Here we can explain how each service works and how they all come together to cover the continuum of care. A display on the floor, showing the

Effect of telehealth on use of secondary care and mortality: findings from the Whole System Demonstrator cluster randomised trial

OPEN ACCESS

Adam Steventon *senior research analyst*[1], Martin Bardsley *head of research*[1], John Billings *associate professor of health policy and public service*[2], Jennifer Dixon *director*[1], Helen Doll *senior research*

Abstract

Objective To assess the effect of home based telehealth interventions on the use of secondary healthcare and mortality.

Design Pragmatic, multisite, cluster randomised trial comparing telehealth with usual care, using data from routine administrative datasets. General practice was the unit of randomisation. We allocated practices using a minimisation algorithm, and did analyses by intention to treat.

Setting 179 general practices in three areas in England.

Participants 3230 people with diabetes, chronic obstructive pulmonary disease, or heart failure recruited from practices between May 2008 and November 2009.

Interventions Telehealth involved remote exchange of data between patients and healthcare professionals as part of patients' diagnosis and management. Usual care reflected the range of services available in the trial sites, excluding telehealth.

Main outcome measure Proportion of patients admitted to hospital during 12 month trial period.

Results Patient characteristics were similar at baseline. Compared with controls, the intervention group had a lower admission proportion within 12 month follow-up (odds ratio 0.82, 95% confidence interval 0.70 to 0.97, P=0.017). Mortality at 12 months was also lower for intervention patients than for controls (4.6% *v* 8.3%; odds ratio 0.54, 0.39 to 0.75, P<0.001). These differences in admissions and mortality remained significant after adjustment. The mean number of emergency admissions per head also differed between groups (crude rates, intervention 0.54 *v* control 0.68); these changes were significant in unadjusted comparisons (incidence rate ratio 0.81, 0.65 to 1.00, P=0.046) and after adjusting for a predictive risk score, but not after adjusting for baseline characteristics. Length of hospital stay was shorter for intervention patients than for controls (mean bed days per head 4.87 *v* 5.68; geometric mean difference –0.64 days, –1.14 to –0.10, P=0.023, which remained significant after adjustment). Observed differences in other forms of hospital use, including notional costs, were not significant in general. Differences in emergency admissions were greatest at the beginning of the trial, during which we observed a particularly large increase for the control group.

Conclusions Telehealth is associated with lower mortality and emergency admission rates. The reasons for the short term increases in admissions for the control group are not clear, but the trial recruitment processes could have had an effect.

Trial registration number International Standard Randomised Controlled Trial Number Register ISRCTN43002091.

Introduction

Efforts worldwide are dealing with the increasing prevalence of chronic disease among an ageing population. The past decade

BMJ 2012;344:e3874 doi: 10.1136/bmj.e3874
(Published 21 June 2012)

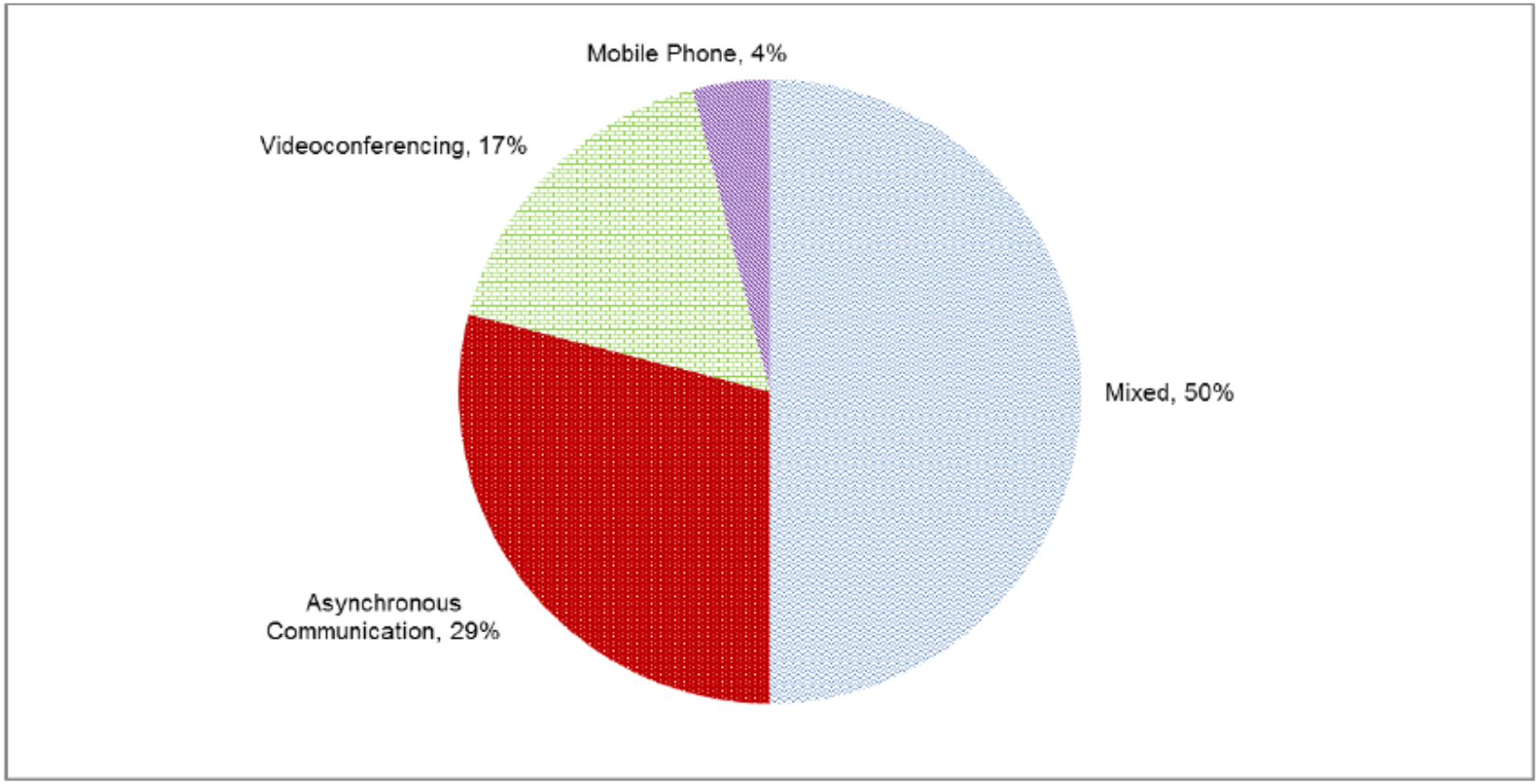
Telehealth: Mapping the Evidence for Patient Outcomes From Systematic Reviews

- The research literature on telehealth is vast and varied, consisting of hundreds of systematic reviews and thousands of studies of use across various clinical conditions and health care functions.
- There is sufficient evidence to support the effectiveness of telehealth for specific uses with some types of patients, including—
    - Remote patient monitoring for patients with chronic conditions;
    - Communication and counseling for patients with chronic conditions;
    - Psychotherapy as part of behavioral health.

For these telehealth applications, the research focus should shift to how to promote broader implementation and address barriers.

- Additional systematic reviews may be helpful for some topics, such as consultation and maternal and child health, where primary studies are available but these have not been synthesized.
- For other uses, such as triage for urgent care, telehealth is cited as offering value but limited primary evidence was identified, suggesting more studies are needed.
- Future research also should assess the use and impact of telehealth in new health care organizational and payment models.

Figure 4. Distribution of telehealth modality across included systematic reviews



Smartphone OS Sales Share (%)

Germany	3 m/e Sep'15	3 m/e Sep'16	% pt. Change
Android	73.9	81.1	7.2
iOS	17.5	15.0	-2.5
Windows	7.6	3.3	-4.3
Other	1.1	0.6	-0.5

GB	3 m/e Sep'15	3 m/e Sep'16	% pt. Change
Android	51.6	55.7	4.1
iOS	38.2	40.6	2.4
Windows	9.8	3.6	-6.2
Other	0.4	0.1	-0.3

France	3 m/e Sep'15	3 m/e Sep'16	% pt. Change
Android	72.3	74.2	1.9
iOS	14.6	19.9	5.3
Windows	12.3	5.2	-7.1
Other	0.8	0.7	-0.1

Italy	3 m/e Sep'15	3 m/e Sep'16	% pt. Change
Android	76.4	82.1	5.7
iOS	10	12.8	2.8
Windows	12.6	4.8	-7.8
Other	1	0.2	-0.8

Spain	3 m/e Sep'15	3 m/e Sep'16	% pt. Change
Android	90.4	93	2.6
iOS	6.3	6.3	0.0
Windows	3	0.7	-2.3
Other	0.4	0	-0.4

USA	3 m/e Sep'15	3 m/e Sep'16	% pt. Change
Android	66.7	63.4	-3.3
iOS	29	34.2	5.2
Windows	3.9	1.9	-2.0
Other	0.4	0.5	0.1

China	3 m/e Sep'15	3 m/e Sep'16	% pt. Change
Android	77.8	85.3	7.5
iOS	18.7	14.2	-4.5
Windows	3.0	0.0	-3.0
Other	0.5	0.4	-0.1

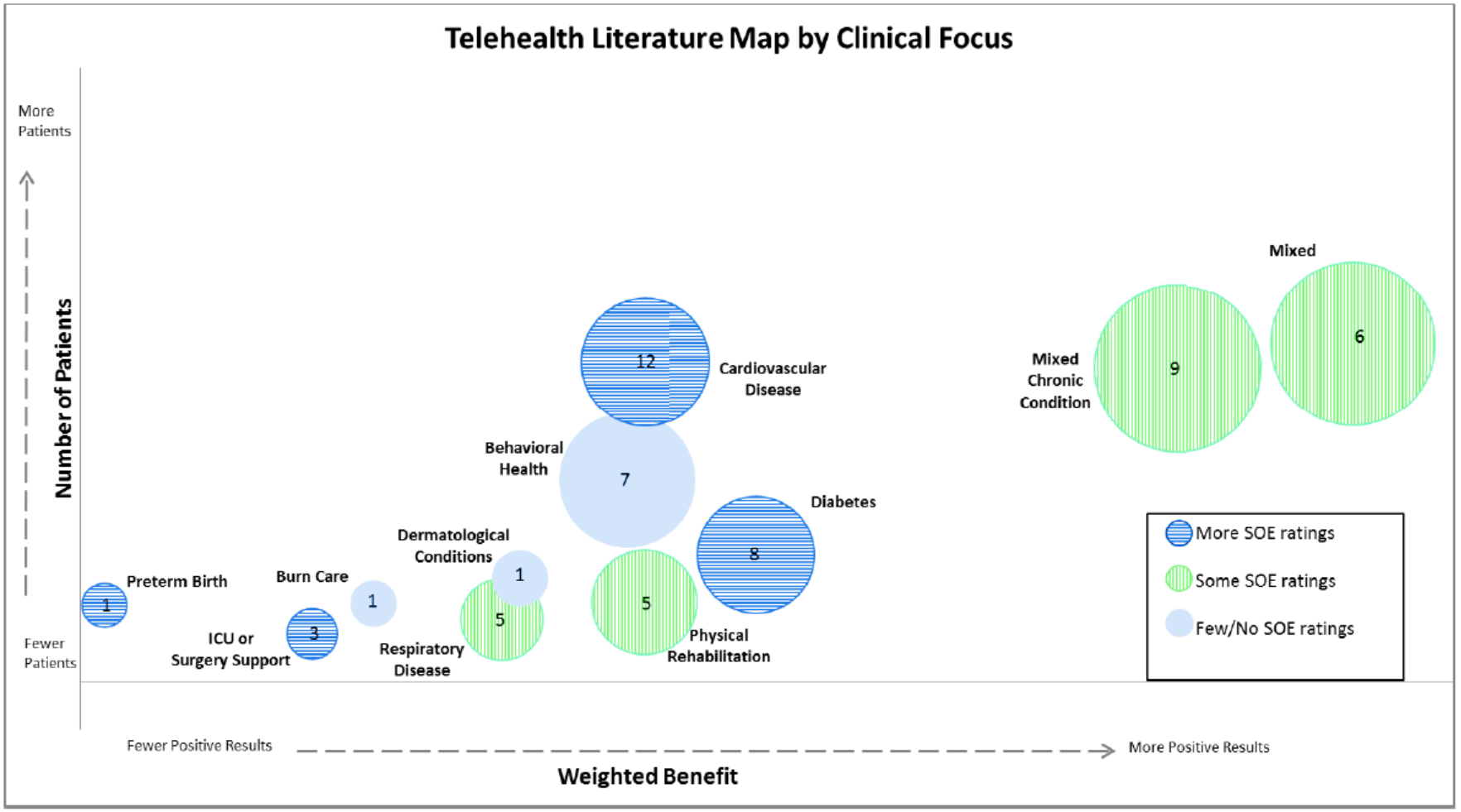
Australia	3 m/e Sep'15	3 m/e Sep'16	% pt. Change
Android	54.5	58.2	3.7
iOS	36.8	37.1	0.3
Windows	7.4	2.3	-5.1
Other	1.3	2.4	1.1

Japan	3 m/e Sep'15	3 m/e Sep'16	% pt. Change
Android	60.7	61.7	1.0
iOS	38.3	37.4	-0.9
Windows	0.5	0.5	0.0
Other	0.5	0.3	-0.2

EU5	3 m/e Sep'15	3 m/e Sep'16	% pt. Change
Android	71.8	76.9	5.1
iOS	18.1	18.9	0.9
Windows	9.4	3.8	-5.6
Other	0.8	0.4	-0.4

Table 2. Characteristics of systematic review evidence by clinical focus and telehealth function

Study Characteristic		Systematic Reviews (N)	Percent of Systematic Reviews by Category	Individual Studies included in Systematic Reviews[a] (N)	Patients[a] (N)
Clinical Focus	Cardiovascular Disease	12	21	121	57,811
	Mixed Chronic Condition	9	15	210	56,276
	Diabetes	8	14	103	16,823
	Behavioral Health	7	12	137	32,770
	Mixed Conditions	6	10	200	61,696
	Physical Rehabilitation	5	9	81	6,715
	Respiratory Disease	5	8	50	3,214
	ICU or Surgery Support	3	5	19	193
	Burn Care	1	2	16	6,782
	Preterm Birth	1	2	15	6,588
	Dermatological Conditions	1	2	24	11,942
	TOTAL for Systematic Reviews by Clinical Focus	**58**		**976[b]**	**260,054**
Telehealth Function	Remote Patient Monitoring	17	29	202	48,321
	Communication and Counseling	14	24	267	95,879
	Multiple Functions	10	17	247	51,684
	Psychotherapy	7	12	114	24,455
	Telerehabilitation	5	9	72	6,281
	Consultation	4	7	53	25,457
	Telementoring	1	2	10	118
	TOTAL for Systematic Reviews by telehealth function	**58**		**965[b]**	**252,195**



a. Bubble size reflects the unduplicated number of individual studies included in the systematic reviews about that clinical focus. The number label on each bubble is the number of systematic reveiws. Smaller bubbles indicate fewer studies, larger bubbles indicate more studies. The color of the bubble represents how many of systematic reviews included strength of evidence assessment.

b. Weighted relative benefit is calculated by weighting the overall conclusion of each review by the number of studies in the review. Bubbles to the right indicate more positive findings while bubbles to the left represent findings that are unclear or found no benefit.

ICU = intensive care unit; SOE = strength of evidence

Category	Topic	Rationale
A	Remote patient monitoring for chronic conditions	Several systematic reviews available, consistent findings of benefit or potential benefit from most reviews
A	Communication and counseling for chronic conditions	Several systematic reviews available, consistent findings of benefit or potential benefit from most reviews.
A	Psychotherapy for behavioral health	Most systematic reviews report benefit or potential benefit; 1 review finds insufficient evidence for use in forensic and correctional psychiatry.
B	Consultation for various clinical reasons	Four reviews addressed telehealth for consultation; three of these did not come to a conclusion. The use of telehealth for consultation crosses clinical areas and may be a viable topic for future synthesis.
B	Applications of telehealth for acute/ICU care including remote patient monitoring and telementoring	The reviews identified for ICU/surgery and burn care combined with reviews in progress in critical care and postoperative care suggest a growing literature base on this important use of telehealth designed to expand access to high tech care in areas where access is limited.
B	Maternal and child health	Pregnancy and newborn routine health care monitoring is a frequent reason for health care visits and access can be limited in some areas. A preliminary search identified studies that cover multiple technologies and uses. A future systematic review may be able to organize the literature in a way that it would be useful for policy and decisionmaking.
C	Triage for urgent and primary care	While this has been proposed as a use for telehealth, most of the identified research was on telephone only interventions. It is unclear if telehealth is not used extensively for this purpose or if it has been used but has not been studied.
C	Applications in pediatrics (managing chronic serious conditions)	Healthcare for children with serious illnesses can be disruptive and impinge on normal life, activities and development. A small number of studies were identified across diverse conditions.
C	Applications relevant to the integration of mental and physical health	Although the integration of mental and physical health is an important goal in many health care reform efforts we did not identify overlap of these topics in telehealth research (e.g., telehealth to address depression in people with diabetes or to help patients struggling with addition to obtain preventive care).
C	Impact of teledermatology on patient outcomes	While there is substantial evidence related to diagnostic concordance, we were unable to identify more than a few studies that included clinical outcomes. While diagnostic concordance is important, research focused on outcomes appears to be needed to inform decisions about this use of the telehealth.
C	Impact on cost and utilization	The evidence on costs is limited and does not correspond to the importance of this issue. Additionally, studies are needed that evaluate telehealth under new payment models.

MEDICAL DEVICES

DEFINIZIONE

- I «medical devices» hanno subito una grande evoluzione: da apparati «isolati» a apparati programmabili via wireless, impiantati, o addirittura costituiti da un software, insomma «connessi»
- **An instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including a component part, or accessory …….intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease**

Prendi decisioni terapeutiche con [redacted] Mobile Continuous Glucose Monitoring System!

CGM ha funzionalità uniche. A differenza degli altri glucometri, che forniscono valori numerici relativi a un singolo momento, CGM offre informazioni sulla glicemia dinamiche, indicando qual è il livello di glucosio attuale, in che direzione si sta muovendo e a che velocità. Inoltre, [redacted] Mobile CGM non richiede prelievi dal polpastrello per la conferma delle decisioni sulla gestione della glicemia.*

* Se gli avvisi di glicemia e le letture glicemiche del sensore non corrispondono ai sintomi o ai valori attesi, occorre effettuare la misurazione tramite prelievo dal polpastrello. La calibrazione richiede almeno due prelievi dal polpastrello giornalieri.

Connettività dei Devices

- Via «FILO»
- Wireless
  - WI-FI
    - 2,4 – 5,0…Ghz
    - Criptato, non criptato
    - Portata 50 metri
  - Bluetooth
    - Di per sè criptato, necessita di ***Pairing***
    - Portata 10 metri (in genere)
- Sistemi wireless a bassa frequenza

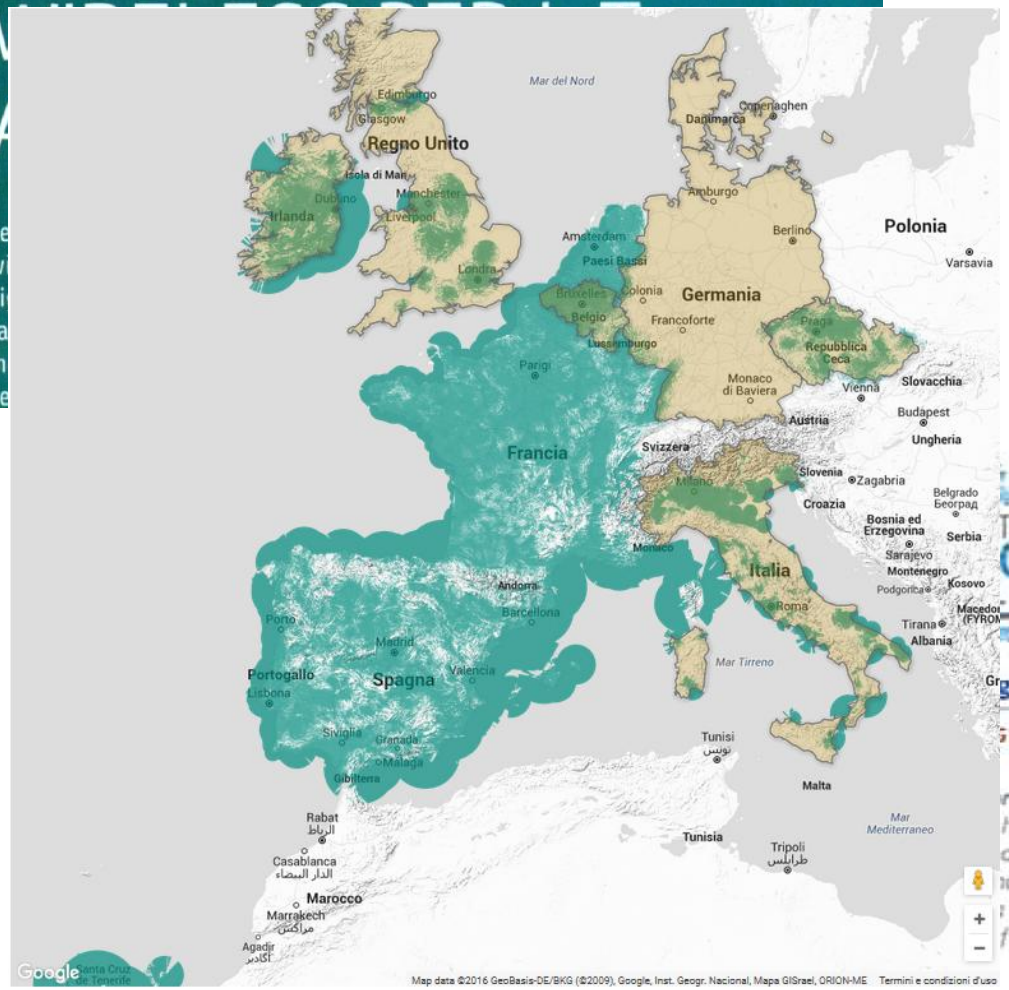
trasmissione dati di prossimità:

NFC

- Near Field Communication (NFC) (in italiano letteralmente “Comunicazione in prossimità”) è una tecnologia che fornisce connettività wireless (RF) bidirezionale a corto raggio (fino a un massimo di 10 cm). È stata sviluppata congiuntamente da Philips, LG, Sony, Samsung e Nokia

trasmissione dati al Cloud:

SIGFOX, LA RETE



getti

GY ENABLERS

ri di chip e
hanno la
di integrare
o dei loro
tecnologia
fox.

Rete NETTROTTER

Network e Connettività

SIGFOX NETWORK OPERATOR

- Consumo energetico molto basso
- Eccellente raggio di azione e sicurezza
- Significativa copertura dell'intero territorio nazionale
- Ottimale per la trasmissione di pochi dati

Piattaforme e Applicazioni

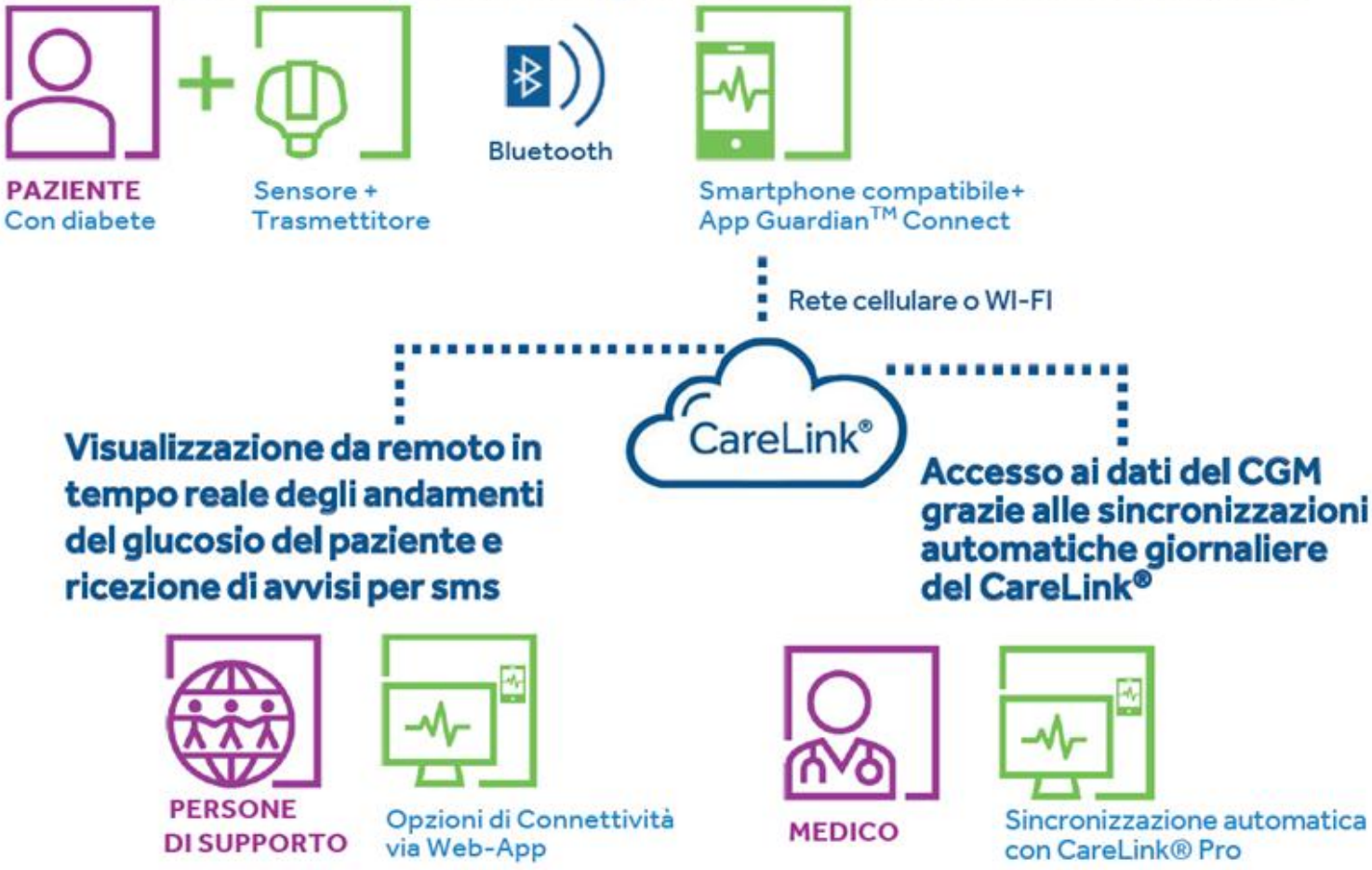
SOLUTION ENABLERS

*Le aziende che implementano **piattaforme ed applicazioni** IoT hanno la possibilità di interfacciarsi con la Rete NETTROTTER.*

Modalità di trasmissione del dato

- App con trasmissione dati *on demand*: condivisione dati con sms, pdf, e-mail watsapp ecc
- App con trasmissione dati in Cloud e consultazione «in remoto»
- App con trasmissione «in continuo» nel Cloud

Controllo in tempo reale dei livelli di glucosio e ricezione automatica di allerte



Previsioni di spesa per «Cybersecurity»

Gartner Says Worldwide IoT Security Spending to Reach $348 Million in 2016

By 2020, More Than 25 Percent of Identified Attacks in Enterprises Will Involve IoT

Worldwide spending on Internet of Things (IoT) security will reach $348 million in 2016, a 23.7 percent increase from 2015 spending of $281.5 million, according to Gartner, Inc. Spending on IoT security is expected to reach $547 million in 2018 (see Table 1). Although overall spending will initially be moderate, Gartner predicts that IoT security market spending will increase at a faster rate after 2020, as improved skills, organizational change and more scalable service options improve execution.

"The market for IoT security products is currently small but it is growing as both consumers and businesses start using connected devices in ever greater numbers," said Ruggero Contu, research director at Gartner. "Gartner forecasts that 6.4 billion connected things will be in use worldwide in 2016, up 30 percent from 2015, and will reach 11.4 billion by 2018. However, considerable variation exists among different industry sectors as a result of different levels of prioritization and security awareness."

Table 1
Worldwide IoT Security Spending Forecast (Millions of Dollars)

2014	2015	2016	2017	2018
231.86	281.54	348.32	433.95	547.20

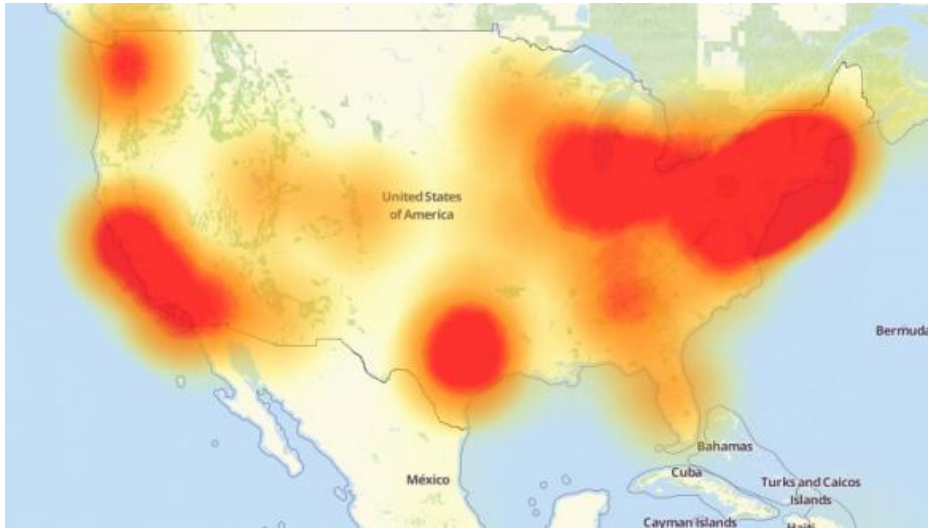
Source: Gartner (April 2016)

Gli *attacchi* a internet

Enorme attacco DDoS piega internet: ecco cosa è successo venerdì 21 ottobre

Numerosi servizi online sono stati inaccessibili per parecchie ore da molte parti del mondo in seguito ad un enorme attacco hacker perpetrato nei confronti di DynDNS

di Nino Grasso pubblicata il **24 Ottobre 2016**, alle **11:00** nel canale SICUREZZA



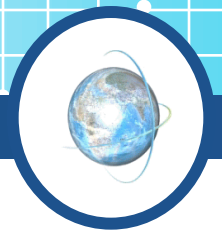
- Quello di venerdì è stato un attacco DDoS, ovvero una particolare tipologia di aggressione in cui si utilizzano varie tecniche per inviare richieste e pacchetti di dati ad un sito internet. L'obiettivo è abusare del traffico a disposizione del sito in modo da saturarlo e rendere difficile la navigazione sullo stesso per tutti gli utenti.
- …. parecchie firme di sicurezza hanno segnalato che **il malware utilizzato all'interno dell'aggressione è Mirai**, il cui codice sorgente è disponibile pubblicamente da circa un mese. Il software malevolo prende di mira dispositivi della Internet of Things, ovvero tutti quei dispositivi tradizionali resi smart dalla capacità di connettersi ad internet, e quindi ad altri dispositivi: ad esempio router, videocamere di sorveglianza.

FSE E LA PRIVACY: CHE DICE IL GARANTE, QUALI RISCHI?

Il processo di migrazione in atto alla sanità elettronica

- Il comma 1 dell'art. 47-bis del d.l. 9 febbraio 2012, n. 5, recante "**Disposizioni urgenti in materia di semplificazione e di sviluppo**", convertito con modificazioni dalla L. 4 aprile 2012, n. 35 ("Semplificazione in materia di sanità digitale") ha sancito la *preminenza* della gestione elettronica rispetto a quella tradizionale per quanto concerne le pratiche cliniche, attraverso l'utilizzo della cartella clinica elettronica così come i sistemi di prenotazione elettronica per l'accesso alle strutture da parte dei cittadini.
- Ha inoltre consentito, a partire dal 1° gennaio 2013, la conservazione anche **soltanto digitale delle cartelle cliniche**.
- Si tratta di uno sviluppo che va visto come ulteriore, decisivo, spostamento in avanti nel processo di migrazione dei servizi sanitari a una gestione (prevalentemente o interamente) informatica.

Le ragioni di opportunità connesse ad una gestione elettronica



- **disponibilità di tutte le informazioni sanitarie con un click e in ogni momento (tendenzialmente 24 ore su 24 e 7 giorni su 7)**
- **accessibilità alle informazioni sanitarie da qualsiasi terminale abilitato**
- completezza informativa
- standardizzazione dei formati
- abbattimento dei costi di archiviazione (*storage*) e dei volumi
- possibilità di verifica degli accessi alle informazioni sanitarie
- automatizzazione dei sistemi di prenotazione delle visite e ritiro dei referti, con abbattimento dei costi e risparmio di tempo per il cittadino
- semplificazione del *workflow* documentale in ambito clinico e amministrativo

il Cloud in Sanità

Cos'è il Cloud?

- "Il Cloud Computing è un ambiente di esecuzione elastico che consente l'accesso via rete e su richiesta ad un insieme condiviso di risorse di calcolo configurabili sotto forma di servizi a vari livelli di granularità.

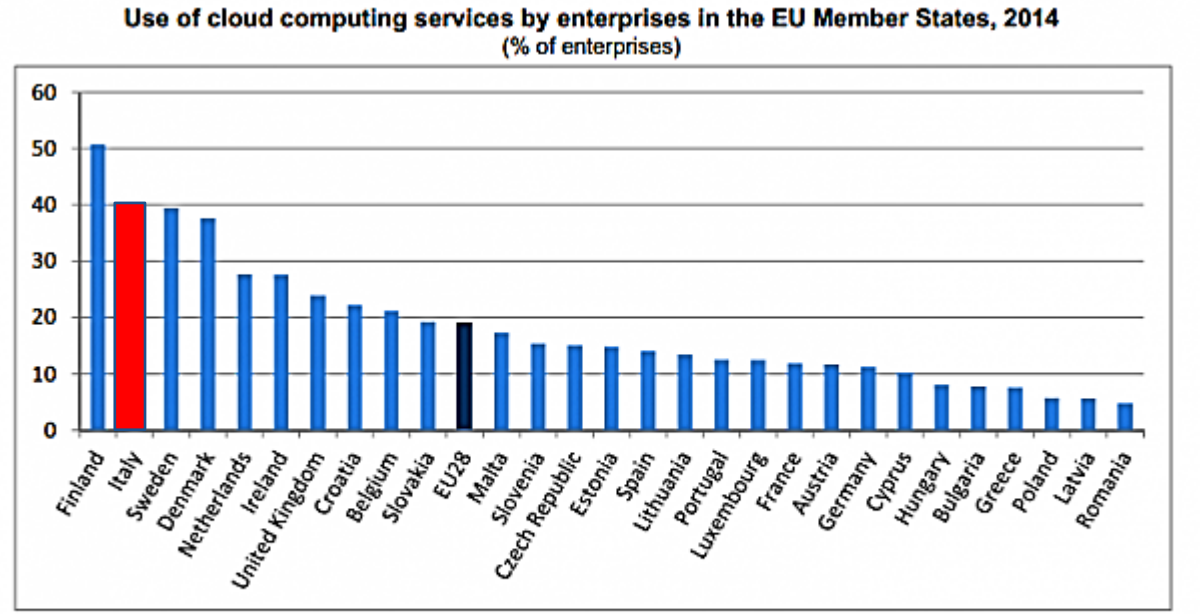
- Tali servizi possono essere rapidamente richiesti, forniti e rilasciati con minimo sforzo gestionale da parte dell'utente e minima interazione con il fornitore"*

L'Italia svetta nel cloud: secondo posto in Europa

29 COMMENTI

di Elena Re Garbagnati, 10 dicembre, 2014 17:32

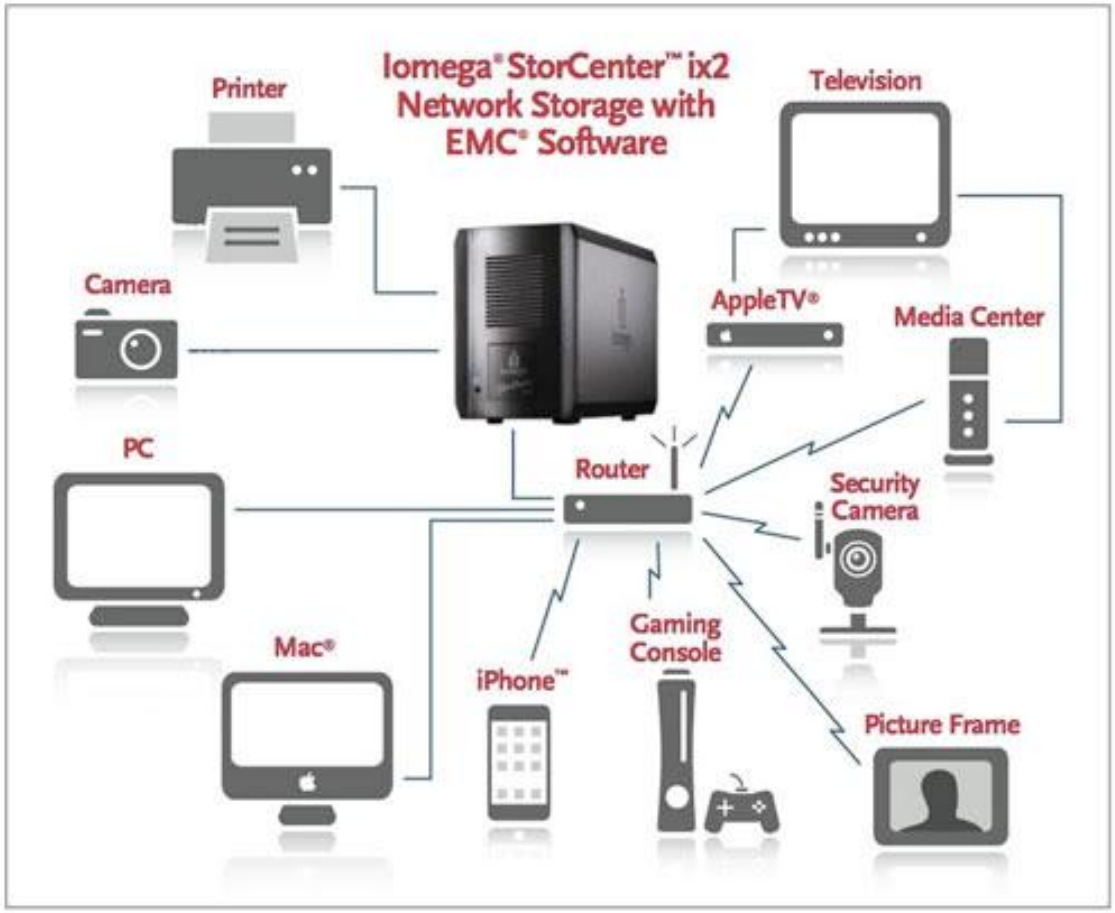
Secondo i dati diffusi da Eurostat il 40% delle aziende italiane sta puntando sul cloud computing e il nostro Paese è il secondo in Europa dopo la Finlandia a sfruttare i servizi cloud. Stefano Sordi di Aruba ci spiega in dettaglio cosa e come sta cambiando in Italia e perché.

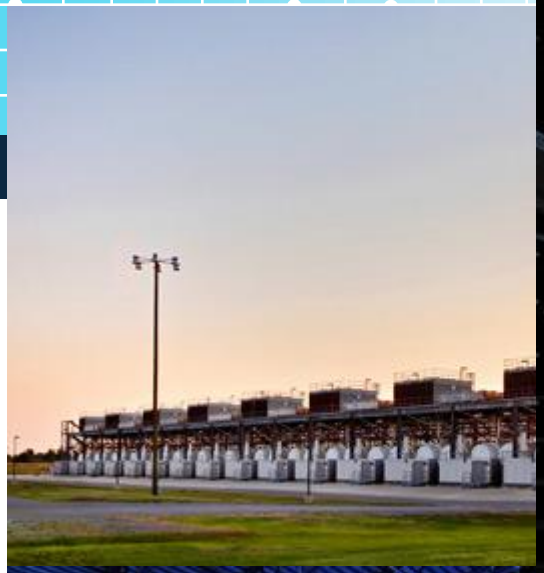


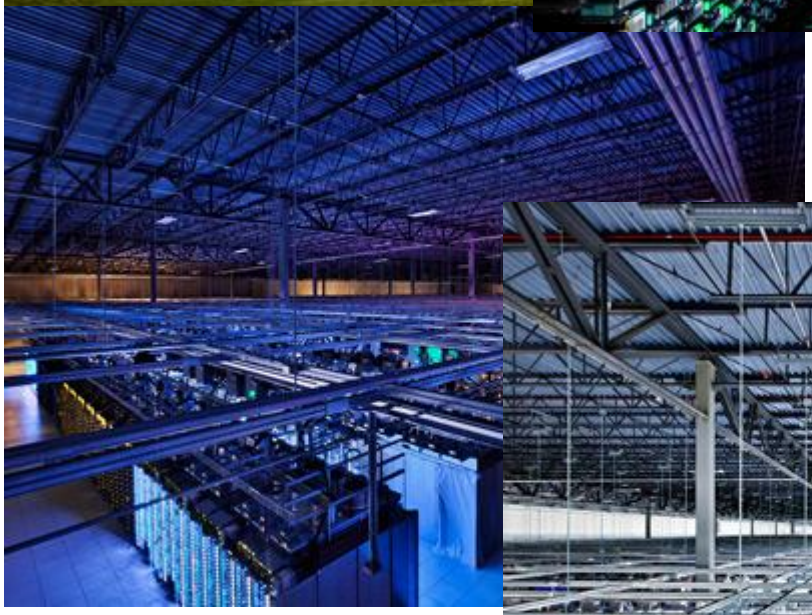
Italia seconda

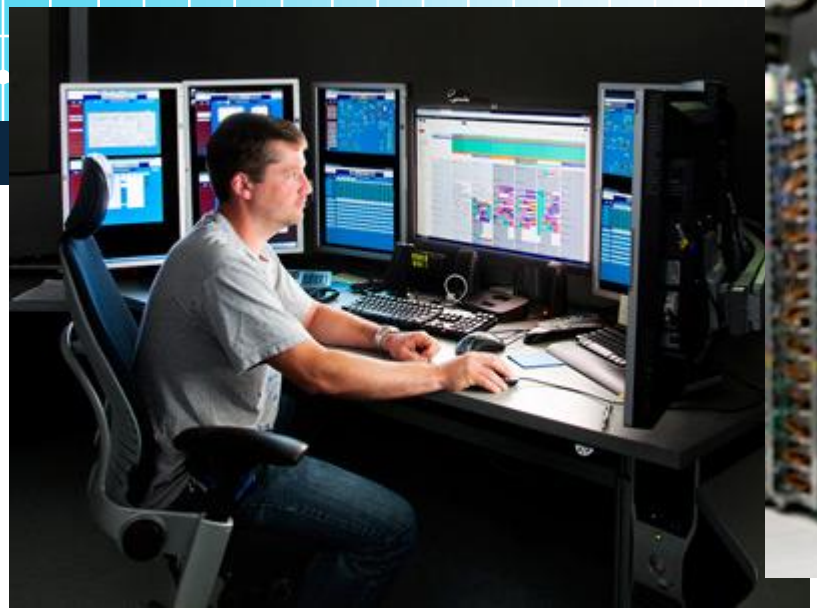
A cosa serve il cloud? Per lo più per la **gestione dei servizi di posta elettronica** (66% su base europea, **86% in Italia**), ma è elevata anche la percentuale di utenze che si affidano alla nuvola per **l'archiviazione di file.** In questo caso la media europea è del 53%, e a fare la parte del leone sono Irlanda (74%), Regno Unito (71%), Danimarca e Cipro (entrambi 70%). In Italia siamo al 32%.

Il «mio» Cloud

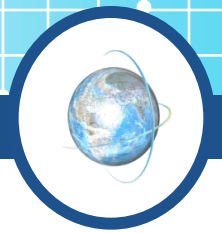

Iomega® StorCenter™ ix2
Network Storage with
EMC® Software
Printer
Television
Camera
AppleTV®
Media Center
PC
Router
Security
Camera
Mac®
iPhone™
Gaming
Console
Picture Frame



Aspetti critici dell'adozione del Cloud

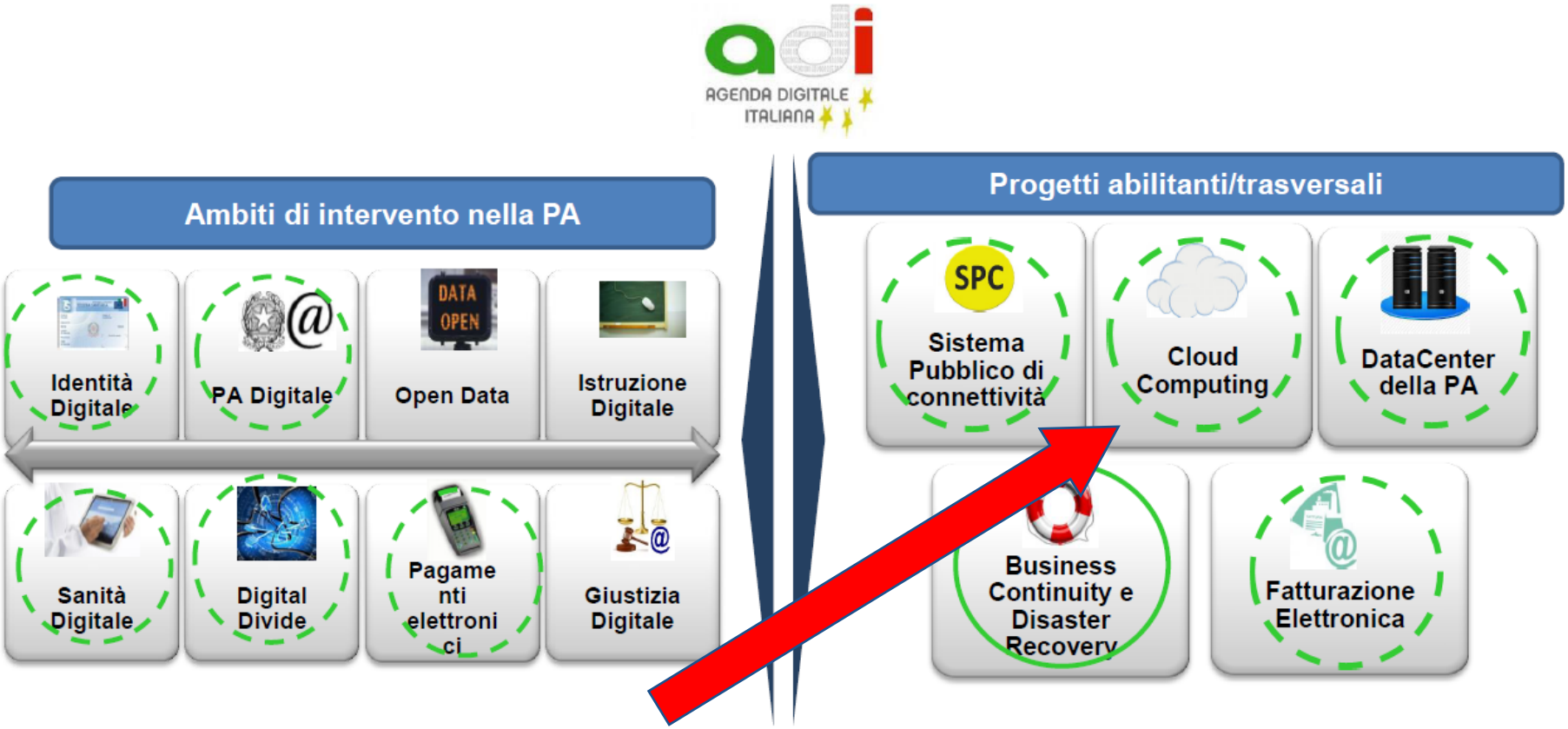


- la sicurezza informatica e la tutela della privacy dei dati sanitari gestiti in ambiente cloud.
- la carenza di normative specifiche che regolamentano l’uso di tale tecnologia nell’erogazione dei servizi sanitari.

Data security measures for the [redacted] Connect Online diabetes management system are designed to ensure your data cannot be viewed or changed by anyone without your permission:

- **Secure storage.** All sensitive data is encrypted and stored in a secure data hosting center. No personal, patient or medical data is stored locally on you or your patient's computers.
- **Encryption.** All linkages between personal and medical data are encrypted at the database level to ensure proper access controls by internal users and external threats.
- **Secure transmissions.** All data transmissions between user and Accu-Chek servers are secured and encrypted in adherence with industry-leading standards.
- **Access authentication.** Accu-Chek Connect Online account access is controlled and validated with strong security and authentication methods; for example, stringent password criteria enforce restrictions on length, require use of both numbers and letters, limit repetition and restrict similarity between passwords and usernames.
- **Separate device and user authentication.** Device level authentication occurs independently of user authentication to ensure system actions performed by a device—such as data upload—are validated separately from actions a user can take, providing additional safeguards to ensure only authorized users can access personal information.
- **Continued monitoring.** External independent security threat analysis and penetration testing is performed. Processes are in place for tracking system modifications and use.

Temi e priorità dell'Agenda Digitale Italiana



Fonte: NetConsulting su fonti varie 2014

La gara Consip per il Cloud nella PA

IL CONTESTO:

Datacenter Pubblici come quelli di Sogei

Datacenter Regionali

SPC - Connettività

Gara Consip per il Cloud nella PA
(24 dicembre 2013)

- **Valore 1,95 md € per cinque anni**
- **Risparmi per la PA 3 md €**

OBIETTIVI per le PA

- *Disporre di servizi IT centralizzati e flessibili,*
- *Disporre di risorse utilizzabili per rispondere a picchi temporanei,*
- *Disporre di risorse utilizzabili per esigenze gestionali*
- *Elevare la sicurezza dei sistemi gestionali pubblici.*

OGGETTO del CLOUD

- *Servizi infrastrutturali informatici*
- *Piattaforme di interazione digitale con cittadini e imprese*
- *Servizi di interoperabilità per i dati e per la cooperazione applicativa*

BENEFICI ATTESI

- *Riduzione tempi di realizzazione dei progetti per eliminazione specifiche gare*
- *Riuso delle applicazioni*
- *Riduzione costi di gestione, amministrativi*

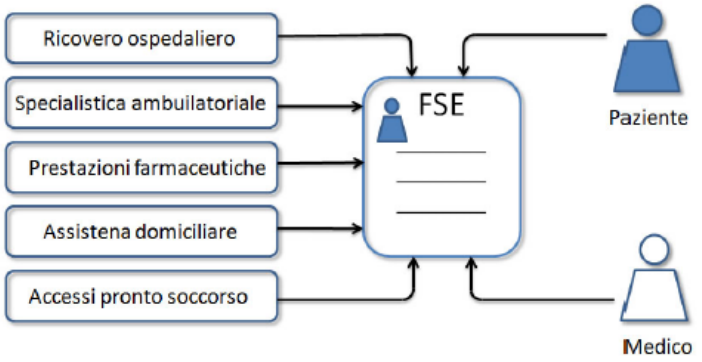
Sanità digitale: linee guida del Fascicolo Sanitario Elettronico

Stato di avanzamento del FSE nelle Regioni italiane

Piena operatività
In avanzata fase di completamento
Sperimentale
Assente

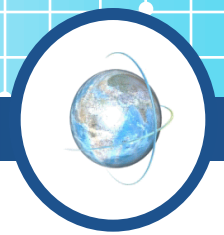
Fonte: Osservatorio Assinform PA (Novembre 2013) e NetConsulting 2014

Linee Guida per la realizzazione del FSE del 31 marzo 2014 emanate da AGID e Ministero della Salute



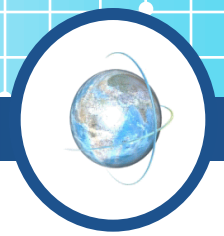
Tempistiche

- Entro il 30 giugno 2014 le Regioni devono predisporre i Piani per realizzare l'archiviazione e la gestione informatica dei documenti sanitari dei cittadini
- Entro il 30 giugno 2015 dovrà essere pienamente operativo il Fascicolo Sanitario Elettronico in tutte le Regioni



- L'adozione del Cloud per la conservazione/elaborazione dei dati personali in Europa comporta l'aderenza alle:
- direttiva 95/46/CE;
- direttiva 2002/58/CE;
- direttiva2006/24/CE.

La direttiva 95/46/CE: costituisce il testo di riferimento, a livello europeo, in materia di protezione dei dati personali.



- **Equilibrio** fra un livello elevato di tutela della vita privata delle persone e la libera circolazione dei dati personali all'interno dell'Unione Europea.

- **Limiti precisi per la raccolta e l'utilizzo dei dati personali** e chiede a ciascuno Stato Membro di istituire un organismo nazionale indipendente incaricato della protezione di tali dati.

- **Il trasferimento dei dati personali da Paesi appartenenti all'Unione Europea verso Paesi non appartenenti all'Unione o allo spazio Economico Europeo, è vietato**, *a meno che il Paese in questione garantisca un livello di protezione «adeguato»*

Localizzazione del Server

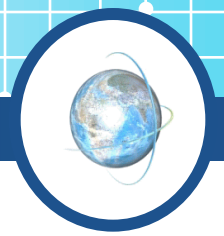
- viene anche espressamente suggerito dal gruppo dei garanti europei di:
- utilizzare servizi FSE (specialmente di storage) localizzati in area UE / SEE o comunque in paesi che rispettino un livello adeguato di protezione dei dati personali
- In ambito cloud si evidenzia pertanto la necessità di appurare contrattualmente quale sia la **localizzazione geografica** dei server utilizzati.

CARTELLA CLINICA ELETTRONICA (EMR / EPR)
Definizione di «Cartella»

- *"Insieme di documenti che registrano un **complesso eterogeneo** di informazioni sanitarie, anagrafiche, sociali, aventi lo scopo di rilevare il percorso diagnostico-terapeutico di un paziente al fine di predisporre gli opportuni interventi sanitari e di poter effettuare indagini statistiche, scientifiche e medico-legali.*
- *È uno strumento informativo **individuale** finalizzato a rilevare tutte le informazioni anagrafiche e cliniche significative relative ad un paziente"*

Sicurezza dei pazienti e gestione del rischio clinico - Manuale per la formazione dei Medici di Medicina Generale e dei Pediatri di Famiglia, marzo 2010, p. 24

Il GARANTE



- **Dossier Sanitario**
  - Va evidenziato che il Garante nelle proprie Linee guida sul FSE, ha distinto concettualmente tra un dossier sanitario del paziente, inteso come complesso di dati sanitari relativi relativi a un paziente trattati all'interno di *un'unica* struttura sanitaria, e il
- **Fascicolo sanitario elettronico**
  - nel quale convergono dossier elaborati da *diverse* strutture sanitarie e dunque rispetto al quale il singolo dossier sanitario rappresenta semplicemente una fonte di popolamento dei dati
- La cartella clinica elettronica va convergendo sempre più nel concetto di fascicolo sanitario elettronico, appare dunque artificioso nell'analisi mantenere una reale separazione tra i concetti.

- *"Il fascicolo sanitario elettronico (FSE) è l'insieme dei dati e documenti digitali di tipo sanitario e sociosanitario generati da eventi clinici presenti e trascorsi, riguardanti l'assistito"* *
- Il FSE è pensato come uno strumento commisurato all'**intera vita del paziente** e ad alimentazione continua nel tempo

art. 12, comma 1 del d.l. 18 ottobre 2012 , n. 179

Il GARANTE

- Il Garante della Privacy ha “scoperto” all'Ospedale Sant'Orsola di Bologna un milione di fascicoli sanitari, leggibili da mille operatori, non tutti medici e infermieri. E ha contestato alla struttura la **mancata acquisizione dei consensi** alla formazione del dossier dei pazienti: questi ultimi ignoravano quali dei propri dati erano nel fascicolo e chi li leggesse. La struttura è stata invitata a raccogliere un ok specifico all’acquisizione dei dossier, e a garantire l’oscuramento di dati ove richiesto dal cittadino, come previsto dalle Linee guida del Garante 2011
- Nel frattempo potrà leggere i fascicoli il solo medico interno che ha in cura il paziente.

DoctorNews del 3 dicembre 2014

Fascicolo sanitario elettronico: aggiornate le specifiche tecniche di interoperabilità

Martedì, 2 Agosto, 2016

Si è concluso il processo di integrazione dei servizi di interoperabilità messi a disposizione delle regioni sull'infrastruttura nazionale

Si è concluso positivamente il processo di integrazione dei servizi di interoperabilità messi a disposizione delle regioni sull'infrastruttura nazionale necessaria a garantire l'interoperabilità dei FSE con il servizio di identificazione degli assistiti attraverso il sistema Tessera Sanitaria.

Con il consolidamento del processo di interoperabilità con le regioni che ad oggi hanno svolto i test, le specifiche tecniche pubblicate il 6 Maggio 2015 hanno quindi subito un processo di riorganizzazione funzionale per dare coerenza all'intero lavoro. Sono state strutturate in modo da avere un master, "Specifiche tecniche per l'interoperabilità tra i sistemi regionali di FSE", che presenta lo scenario architetturale di riferimento e i principali processi di interoperabilità necessari e previsti in sede di prima implementazione del FSE, e una serie di allegati che mirano a dettagliare nello specifico la particolare materia di riferimento:

A – Processi di business

B – Framework e dataset dei servizi base

C – Affinity Domain Italia

D – Identificazione di un assistito

E – Servizi di identificazione

F – Configurazione delle Porte di Dominio

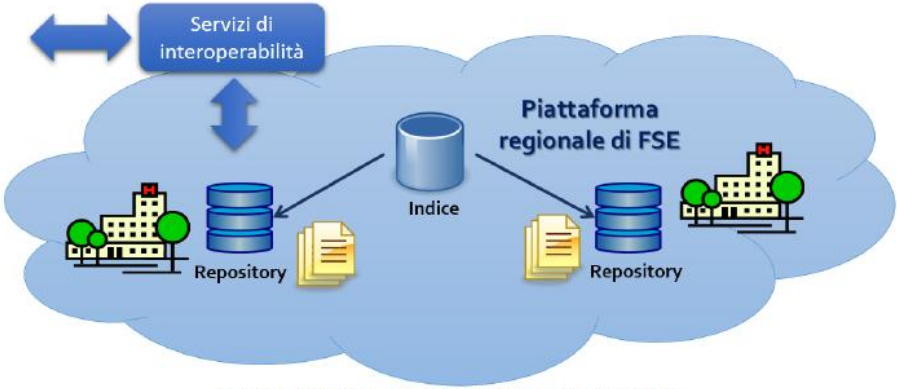


Figura 1. Architettura di una piattaforma regionale di FSE

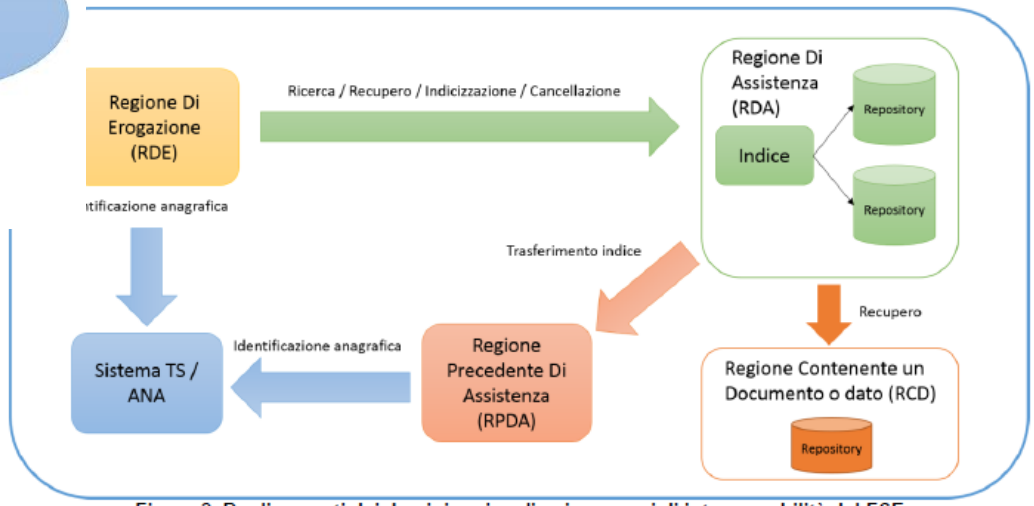


Figura 2. Ruoli assunti dai domini regionali nei processi di interoperabilità del FSE

Costruzione asserzione di attributo	
Nodo	RDE
Descrizione	La presente attività ha lo scopo di costruire una asserzione di sicurezza necessaria per effettuare l'operazione. Essa comprende una serie di attributi, quali l'identificativo ed il ruolo dell'utente, il tipo di richiesta, l'identificativo dell'assistito oggetto della richiesta, il contesto operativo della richiesta, l'identificativo del dominio regionale richiedente, e così via. L'asserzione di attributo, la cui validità temporale deve essere limitata, deve essere firmata dalla RDE.

2.1. Messaggio di richiesta

```
<soapenv:Envelope
      xmlns:soapenv="http://www.w3.org/2003/05/soap-envelope"
      xmlns:add="http://www.w3.org/2005/08/addressing"
      xmlns:urn="urn:oasis:names:tc:SAML:2.0:protocol"
      xmlns:urn1="urn:oasis:names:tc:SAML:2.0:assertion">
   <soapenv:Header>
      <add:To xmlns="http://www.w3.org/2005/08/addressing">
           https://wscoop.sanita.finanze.it/FSEIdentityAssertionWeb/services/I
           dentityAttributeQueryService
      </add:To>
     <Action xmlns="http://www.w3.org/2005/08/addressing">
           urn:mef:IdentityAttributeQuery
      </Action>
     <add:MessageID>uuid:db221ad7-9ef7-4220-bafa-1a79e137e13f</add:MessageID>
      <ReplyTo xmlns="http://www.w3.org/2005/08/addressing">
    <Address>http://www.w3.org/2005/08/addressing/anonymous</Address>
</ReplyTo>
<add:FaultTo>
           <add:Address>
           http://www.w3.org/2005/08/addressing/anonymous
        </add:Address>
        </add:FaultTo>
   </soapenv:Header>
   <soapenv:Body>
      <urn:AttributeQuery ID="f7ca8a71-b154-4ce3-9562-cc82e540eacf"
Version="2.0" IssueInstant="2016-07-15T10:16:19.798+01:00">
          <urn1:Subject>
            <urn1:NameID NameQualifier="2.16.840.1.113883.2.9.4.3.2">
                  PMNTST59A01L317O
            </urn1:NameID>
          </urn1:Subject>
        </urn:AttributeQuery>
```

- La creazione del Dossier e del Fascicolo Sanitario Elettronico (FSE) è facoltativa ed essi possono essere **attivati solo con consenso specifico ulteriore dell'interessato.**
- Il provvedimento del Garante n.331 del **4 giugno 2015** contiene le linee guida in materia di dossier sanitario, pubblicate in allegato A in Gazzetta Ufficiale n.164 del 17 luglio 2015 che affermano a pag. 22: "**L'interessato deve essere informato che l'eventuale mancato consenso al trattamento dei dati personali mediante il dossier sanitario non incide sulla possibilità di accedere alle cure mediche richieste**." e a pag.27
- in caso di revoca del consenso: "Le informazioni sanitarie presenti devono restare disponibili al professionista o alla struttura interna al titolare che le ha redatte e per eventuali conservazioni per obbligo di legge (art. 22, comma 5, del D.Lgs 196/2003), ma non devono essere più alimentate e condivise con altri professionisti degli altri reparti che prenderanno in seguito in cura l'interessato".

- Con l'art.4 dell'ACN **17/12/2015 la compartecipazione degli specialisti ambulatoriali alla realizzazione dei flussi informatici aziendali è divenuta un dovere contrattuale ordinario**. Secondo le linee guida del Garante n.21 del 25 giugno 2009, la refertazione on-line è regolamentata dal DPCM 8 agosto 2013 (in GU n.243 del 16 ottobre 2013) che prevede la messa a disposizione per l'assistito del SSN del referto digitale o copia cartacea e all'art. 2 prevede per il referto digitale **l'obbligo di firma digitale o elettronica** ai sensi degli artt. 21 e 24, comma 2, D.Lgs n.82/2005 (CAD = Codice Amministrazione Digitale).
- Per l'accesso online ai referti è dunque necessario che:
- a. il referto sia firmato digitalmente dallo specialista,
- b. l'assistito abbia dato il consenso al FSE all'azienda,
- c. il consenso sia stato registrato al sistema informatico dedicato da parte degli operatori aziendali affinchè l'azienda che ha erogato la prestazione renda visibile il referto anche al MMG/PLS curante dell'assistito.

Oscuramento selettivo di dati sanitari

- L'interessato ha inoltre la possibilità di "**oscurare**" alcuni dati sanitari, ossia decidere (anche evidentemente in via preventiva) che non compaiano nel FSE.
- Può trattarsi ad esempio dell'esito di una singola visita specialistica o dell'assunzione di un farmaco
- Il sistema software di gestione del FSE **deve pertanto essere strutturato in maniera tale da consentire questo livello di decisione da parte dell'interessato**, la cui scelta può sempre essere reversibile (per cui l'interessato deve poter vedere, lui solo, l'intero contenuto del FSE e decidere a quali soggetti concedere i privilegi informatici per visualizzare determinate informazioni. L'oscuramento perciò dovrebbe poter essere selettivo).
- L'interessato può decidere in definitiva *"se e quali dati relativi alla propria salute non devono essere inseriti nel fascicolo medesimo"* (art. 12, co. 3-bis d.l. 179/12).

Oscuramento dell'Oscuramento

- È altresì prevista la possibilità di non rendere neppure conoscibile (anche solo ad alcuni soggetti) la scelta dell'interessato di oscurare alcune informazioni. Il Garante sul punto ha parlato di "**oscuramento dell'oscuramento**"
- Anche questa forma di privacy (eventualmente limitata solo ad alcuni dei soggetti che possono accedere al FSE) deve essere considerata quando si sviluppa un'applicazione informatica per la gestione del FSE
- Il Garante ha comunque evidenziato che *«l'accesso al FSE/dossier deve essere sempre consentito al soggetto che ha redatto il documento con riferimento all'interessato medesimo»*
- Sembra che l'oscuramento (come anche l'oscuramento dell'oscuramento) non possa operare nei confronti del personale sanitario che alimenta il FSE, limitatamente ai documenti apportati in via *diretta*

123456

LA PASSWORD...QUESTA (S)CONOSCIUTA

Le password più usate

1. password
2. 123456
3. 12345678
4. abc123
5. qwerty
6. monkey
7. letmein
8. dragon
9. 111111
10. baseball
11. iloveyou
12. trustno1
13. 1234567
14. sunshine
15. master
16. 123123
17. welcome
18. shadow
19. ashley
20. football
21. jesus
22. michael
23. ninja
24. mustang
25. password1

Esempio di Password valida

- C!SA,eh35a.Vb?
- Msln78,c110eL!
- 14 caratteri
- Maiuscole e minuscole
- Numeri
- Segni di interpunzione

Come creare una password «sicura»

- pensa a un’intera frase facile da ricordare e poi usa solo l’inizio di ogni parola, mantenendo intatta la punteggiatura. Esempio: «Ciao! Sono Alberto, e ho 35 anni. Vuoi ballare?» La password sarà: «**C!SA,eh35a.Vb?**»
- «Mi sono laureato nel 78, con 110 e Lode!»: La password sarà: «**Msln78,c110eL!**»

Come vengono memorizzate

- Nome Utente: PincoPallino
- Password: Il Migliore!

- **HASH**: «Ahf%4964O,3j2T»

Comportamenti …a rischio

Le tecniche di attacco

Ma come fa un pirata a scoprire una delle nostre password? Esistono diverse possibilità, ma le due più comuni sono quasi banali: può provare tutte le combinazioni possibili di lettere e numeri fino a trovare quella giusta oppure può con qualche trucco convincere noi stessi ad inviargliela. La prima possibilità è il cosiddetto brute force: il metodo è di per sé infallibile, perché è ovvio che provando tutte le com binazioni possibili prima o poi si trova quella giusta, a prescindere da quanto complicata possa essere la password. Tuttavia è un metodo che richiede molto tempo: ecco, dunque, che la robustezza della password è fondamentale. Infatti, una password troppo corta e facile, come "1234" oppure "alligatore3", viene scoperta molto rapidamente da un meccanismo di brute force, soprattutto se abbinato ad un dizionario (significa che prima di tentare le combinazioni casuali si provano delle combinazioni di numeri e parole molto comuni).

Ingegneria sociale

La seconda opzione è più frequente di quanto si possa immaginare e prevede di perpetrare il furto delle credenziali utilizzando attacchi di tipo phishing. In poche parole, usando sofisticate tecniche di ingegneria sociale, i malfattori provano a convincerci a fornire loro i nostri dati personali. Sembra impossibile, eppure negli ultimi tempi questa particolare tecnica di attacco sta dando molte "soddisfazioni" ai pirati! Ci è mai capitato di ricevere un'e-mail da parte di qualcuno che fingeva di essere il gestore di uno dei siti Web a cui siamo registrati, nella quale veniva chiesto di rispondere indicando nome utente e password per svolgere una qualche forma di test? Probabilmente abbiamo cestinato immediatamente il messaggio di posta elettronica in questione, riconoscendo la truffa. Ma se questo tipo di e-mail è ancora in circolazione significa che ci sono ancora molte persone che "abboccano" alla trappola: nessun tipo di truffa continua ad essere perpetrata se non produce frutti. Combattere questo tipo di furti di password è abbastanza semplice: basta ricordarsi sempre che nessun gestore di un sito Web (che sia quello della nostra banca, dell'assicurazione o del negozio online) ci chiederà mai di indicare le nostre credenziali via e-mail o su siti Web diversi dal suo sito ufficiale

COME NON FARSI RUBARE LA PASSWORD!

Nessuno può considerarsi al sicuro da un furto di password ed è per questo motivo che è importante prendere delle semplici precauzioni per evitare che ciò possa crearci grandi problemi.

1. Creare diversi indirizzi e-mail

Uno da non comunicare a nessuno e da utilizzare solo per iscriversi a siti Internet importanti (Amazon, eBay, PayPal eccetera); un altro da usare per iscriversi a siti di vario genere (blog, forum on-line...); e almeno un terzo indirizzo da comunicare ad amici e colleghi per mantenersi in contatto. In questo modo, una eventuale perdita di credenziali degli account più "pubblici" non intaccherà realmente la sicurezza di ciò che conta davvero.

2. Impostare un numero di telefono per recuperare la password

Un pirata che riesce a scoprire la password di un nostro account importante per prima cosa la modifica, in modo da impedirci l'accesso. Solitamente, però, non può modificare il numero di telefono associato all'account e grazie ad esso potremo recuperare l'account stesso.

3. Crittografare i file importanti

Se siamo abituati a usare servizi come Google Drive per caricare on-line dei file confidenziali, ci conviene crittografarli prima di inviarli su Internet (meglio se con un programma come Cryptophane: www.winmagazine.it/link/3611). In questo modo, un eventuale malintenzionato non potrebbe comunque leggerli.

4. Non archiviare mai le password in chiaro

Qualcuno ha l'abitudine di inviarsi tramite e-mail dei messaggi contenenti le password di accesso ai siti ai quali si registra. È una pessima idea! Se qualcuno riuscisse ad entrare nell'account e-mail avrà accesso automatico anche agli altri siti.

5. Non caricare sul Web di tutto e di più

Ricorda che ciò che carichi sul Web non è più da considerare privato (alcune tue immagini potrebbero diventare di pubblico dominio contro il tuo volere e un tuo stato "privato" su Facebook potrebbe essere letto da altri). In altre parole, se una cosa è privata non caricarla sul Web, a prescindere dalle promesse di garanzia della privacy del sito Web o del gestore di storage on-line.

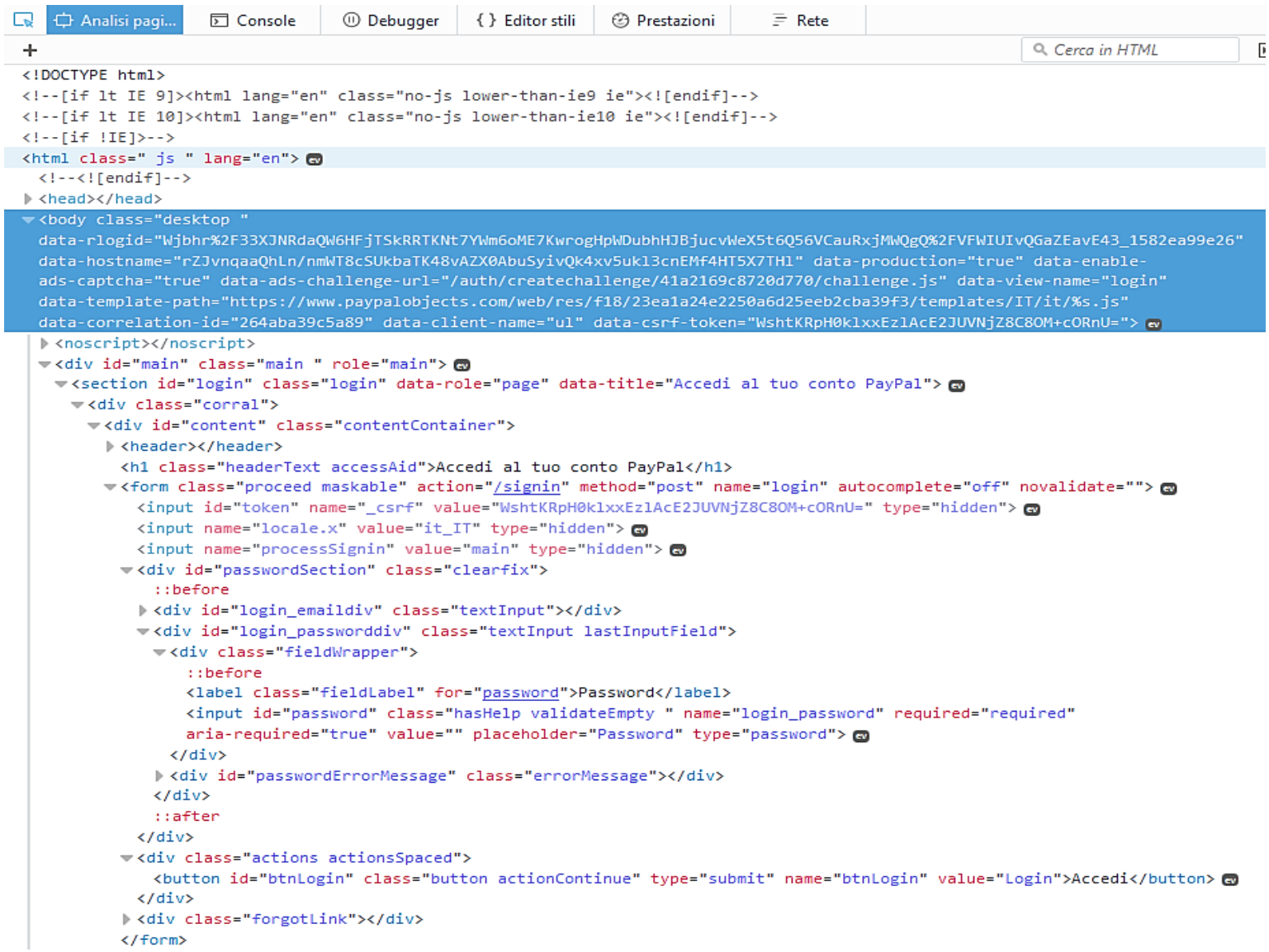
pincopallino@pincopallino.com

••••••••••••

Accedi

Problemi di accesso?

Registrati


Analisi pagi...
Console
Debugger
Editor stili
Prestazioni
Rete
Cerca in HTML
<!DOCTYPE html>
<!--[if lt IE 9]><html lang="en" class="no-js lower-than-ie9 ie"><![endif]-->
<!--[if lt IE 10]><html lang="en" class="no-js lower-than-ie10 ie"><![endif]-->
<!--[if !IE]>-->
<html class=" js " lang="en">
<!--<![endif]-->
<head></head>
<body class="desktop "
data-rlogid="Wjbhr%2F33XJNRdaQW6HFjTSkRRTKNt7YWm6oME7KwrogHpWDubhHJBjucvWeX5t6Q56VCauRxjMWQgQ%2FVFWIUIvQGaZEavE43_1582ea99e26"
data-hostname="rZJvnqaaQhLn/nmWT8cSUkbaTK48vAZX0AbuSyivQk4xv5ukl3cnEMf4HT5X7TH1" data-production="true" data-enable-
ads-captcha="true" data-ads-challenge-url="/auth/createchallenge/41a2169c8720d770/challenge.js" data-view-name="login"
data-template-path="https://www.paypalobjects.com/web/res/f18/23ea1a24e2250a6d25eeb2cba39f3/templates/IT/it/%s.js"
data-correlation-id="264aba39c5a89" data-client-name="ul" data-csrf-token="WshtKRpH0klxxEzlAcE2JUVNjZ8C8OM+cORnU=">
<noscript></noscript>

<section id="login" class="login" data-role="page" data-title="Accedi al tuo conto PayPal">

<header></header>
<h1 class="headerText accessAid">Accedi al tuo conto PayPal</h1>
<form class="proceed maskable" action="/signin" method="post" name="login" autocomplete="off" novalidate="">
<input id="token" name="_csrf" value="WshtKRpH0klxxEzlAcE2JUVNjZ8C8OM+cORnU=" type="hidden">
<input name="locale.x" value="it_IT" type="hidden">
<input name="processSignin" value="main" type="hidden">

::before

::before
<label class="fieldLabel" for="password">Password</label>
<input id="password" class="hasHelp validateEmpty " name="login_password" required="required"
aria-required="true" value="" placeholder="Password" type="password">

::after

<button id="btnLogin" class="button actionContinue" type="submit" name="btnLogin" value="Login">Accedi</button>

</form>

pincopallino

••••••••••••••

Accedisecicredi

Problemi di accesso?

Registrati se credi o non credi

- Considerare la possibilità di accesso con doppia autenticazione per servizi *critici*
  - Gmail
  - DropBox
  - PayPal
- Consiste nella conferma, con un codice inviato per SMS e da inserire subito, dell'effettivo accesso da parte del proprietario
- Per alcuni Provider, è possibile «autenticare» una volta per tutte un dispositivo. Quindi un accesso a Gmail da un PC «diverso» (p. es. in USA) va confermato: ciò aumenta la comodità ma riduce un pò la sicurezza

Ricevi un SMS

Riceverai un SMS con un codice speciale. Indica a quale numero vuoi ricevere l'SMS.

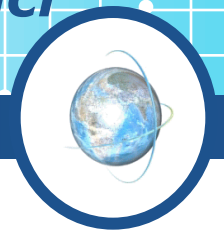
xxxxxxxxx[redacted]

Non hai il telefono cellulare a portata di mano? **Prova un altro metodo**

Desidero ricevere l'SMS

COME CI RUBANO LE PASSWORD

Phishing: Ecco le cinque truffe più popolari ed efficaci



Resetta la tua password

- Si ricevono delle false notifiche via e-mail, social media o programma di messaggistica istantanea in cui si viene avvisati che nostro account è stato hackerato e che bisogna resettare la password. A questo punto si può trovare un link sul quale cliccare o addirittura un file allegato da usare per il "reset". Chi cade nel tranello d'aprire l'allegato infetta di solito il pc con qualche malware progettato per rubare password e numeri di carta di credito

False prenotazioni da «confermare»

- di solito c'è un link che spedisce l'utente su siti dannosi contenenti codici in grado di entrare nel computer della vittima

Vacanze ed eventi funesti

Sei in un video

- Per visualizzare hai necessità di scaricare un update..

Sito sicuro ma con link pericolosi

Fonte: Kapersky Labs

Truffe su Watsapp ®

La truffa del buono sconto da Zara

- *"Rispondi al nostro semplice sondaggio e vinci un buono da **150 euro** da **Zara***", questo il messaggio visualizzato e si tratta ovviamente di una truffa. Cliccando infatti sul **link**, l'utente viene indirizzato verso una serie di passaggi per sottoscrivere un **abbonamento** che consuma il **credito**. Ovviamente senza rendersene conto. In questo caso bisogna contattare immediatamente il **gestore** telefonico per comunicare la **disdetta**.

WhatsApp è scaduto

- Può capitare durante la navigazione di visualizzare un messaggio **pop up** che ci informa che il nostro abbonamento alla app sta per **scadere**. Si tratta di un'altra truffa, di cui la Polizia Postale spiega il funzionamento e le conseguenze. *"Il messaggio chiede di inserire il **proprio numero** di telefono, ma facendolo, invece che sottoscrivere un abbonamento all'applicazione di messaggistica, se ne attiva uno da **20 euro** che invia **sfondi** per il cellulare"*. In questo caso basta **spegnere** il telefono e **riavviarlo**.

WhatsApp Gold

- *"Una promessa di un servizio esclusivo, dietro alla quale si nasconde un **malware***", così viene definita la terza truffa veicolata da WhatsApp. **Diffidare** quindi da questo messaggio: *"Hey, finalmente è arrivata la **versione segreta** di WhatsApp. Questa versione – la Gold – è usata solo da grandi celebrità. Ora puoi usarla anche tu"*. Quello che accade nel caso in cui si scarichi l'**upgrade** è infatti che il telefono venga infettato da un malware, che permette agli **hacker** di controllare lo **smartphone**.

La truffa delle emoticon

- Due **virus** invitano gli utenti a **scaricare** nuove **emoticon**: la Polizia Postale ci ricorda che nessun aggiornamento delle "faccine" viene segnalato tramite messaggio, ma solo con gli aggiornamenti delle applicazioni.

Il messaggio audio inesistente

- Evitare di aprire qualsiasi messaggio che segnali la presenza di una **nota audio** in segreteria, e che provenga da **indirizzi** strani. Si tratta infatti di un virus che accede al **controllo** delle app installate, come **fotocamera** o galleria fotografica: la truffa prevede poi che l'utente venga **ricattato** con richieste di denaro per foto considerate "delicate".

Fonte: Polizia Postale

Rita Caperna publicita@miglioritariffe.online tramite tin.it
10 nov (1 giorno fa)
a l.decandia

Fai attenzione a questo messaggio. Messaggi di questo tipo sono stati utilizzati per carpire i dati personali delle persone. Se il mittente non è una persona di tua fiducia, non fare clic sui link e non rispondere fornendo dati personali. Ulteriori informazioni

ATTENZIONE! Se tu o un tuo caro soffre di diabete, queste saranno le righe più importanti che potrai mai leggere... Scopri Come Migliaia di Persone Hanno Già Utilizzato il Sistema Guarire il Diabete™ per Guarire Completamente dal Diabete in Meno di Tre Settimane!

Adesso fai questo:

Click Qui

Siediti, chiudi la porta a chiave, stacca il telefono... e leggi questo report per scoprire come stimolare il tuo pancreas a produrre più insulina giorno dopo giorno...

Ascolta da rinomati scienziati e specialisti del diabete e impara come ridurre l'uso di farmaci e abbassare i livelli di glucosio nel sangue in modo naturale e sicuro.

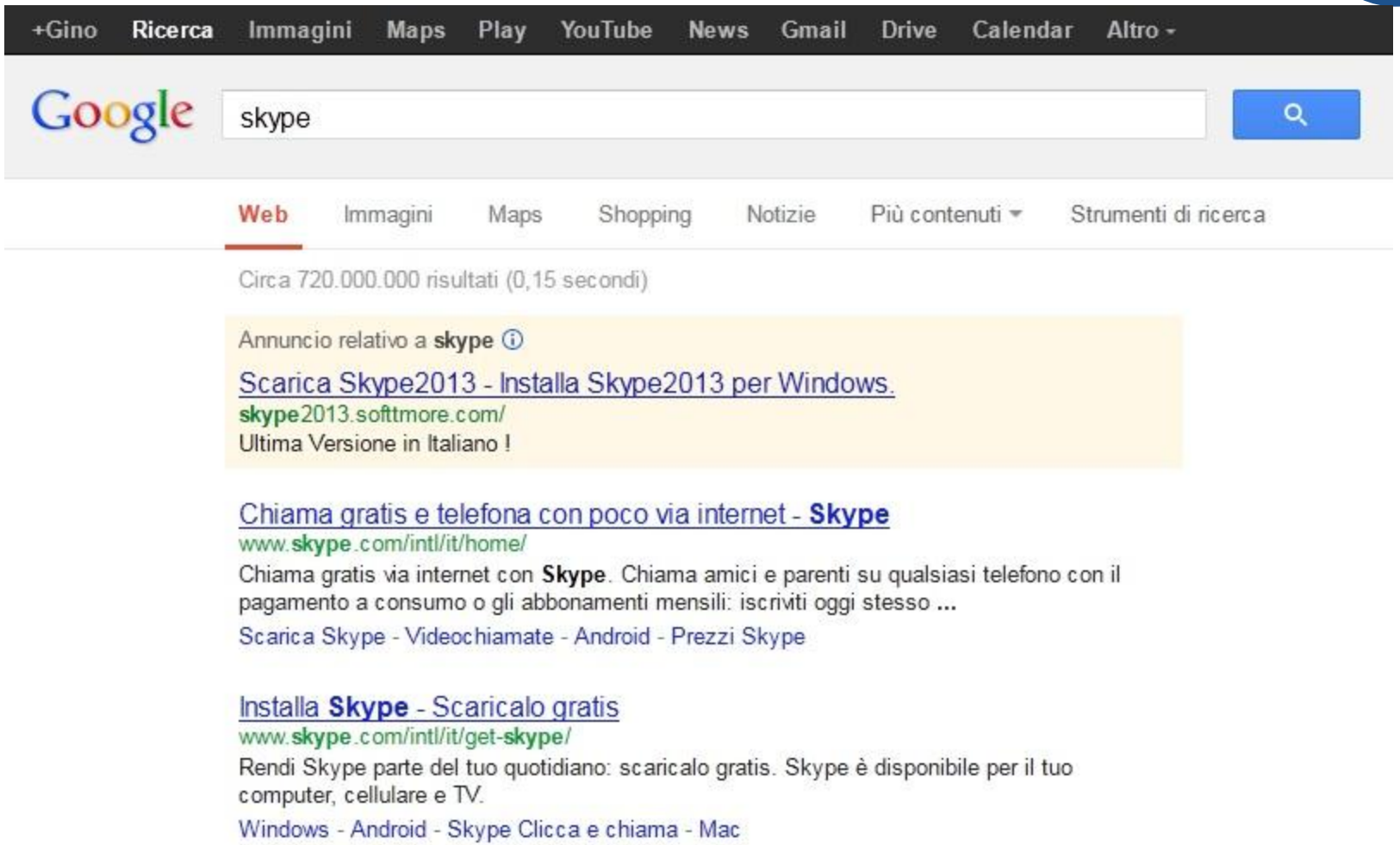
Click Qui

Normalizzare il tasso di zucchero nel sangue agendo direttamente sul funzionamento del pancreas.
Ripristinare la funzione del pancreas ed eliminare la resistenza all'insulina.
Prevenire o far regredire le complicanze del Diabete.
Eliminare la necessità di prendere farmaci diabetici.
Rinforzare il sistema immunitario migliorando notevolmente lo stato di salute.

Click Qui

Il Risultato?

- Furto di dati sensibili…
  - Furto di identità
  - Furto di dati finanziari
    - Password CC, numero Carta di Credito ecc.
- *Cattura* del PC
  - Creare BotNet
  - Effettuare attacchi Ddos
- Attivazione di abbonamenti a Servizi


+Gino Ricerca Immagini Maps Play YouTube News Gmail Drive Calendar Altro
Google
skype
Web Immagini Maps Shopping Notizie Più contenuti Strumenti di ricerca
Circa 720.000.000 risultati (0,15 secondi)
Annuncio relativo a skype
Scarica Skype2013 - Installa Skype2013 per Windows.
skype2013.softtmore.com/
Ultima Versione in Italiano !
Chiama gratis e telefona con poco via internet - Skype
www.skype.com/intl/it/home/
Chiama gratis via internet con Skype. Chiama amici e parenti su qualsiasi telefono con il pagamento a consumo o gli abbonamenti mensili: iscriviti oggi stesso ...
Scarica Skype - Videochiamate - Android - Prezzi Skype
Installa Skype - Scaricalo gratis
www.skype.com/intl/it/get-skype/
Rendi Skype parte del tuo quotidiano: scaricalo gratis. Skype è disponibile per il tuo computer, cellulare e TV.
Windows - Android - Skype Clicca e chiama - Mac

HOME | ASSISTENZA

skype

SCARICA

skype

Milioni di persone utilizzano Skype

Unisciti ai milioni di persone in tutto il mondo che utilizzano Skype per mantenersi in contatto. Sicuramente su Skype troverai persone che conosci.

Sfrutta le tariffe economiche per le chiamate telefoniche

Con Skype puoi chiamare familiari e amici in qualsiasi parte del mondo si trovino. Puoi acquistare credito Skype che ti verrà scalato durante la conversazione o scegliere un piano mensile per utilizzare le tariffe migliori.

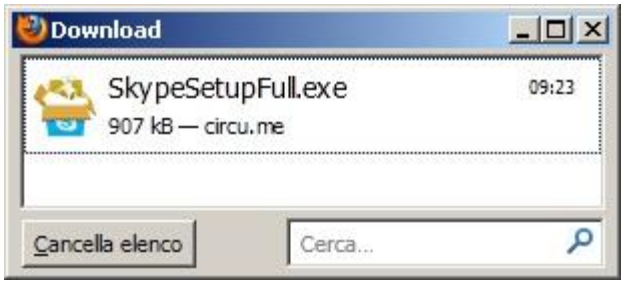
Facile da scaricare e installare

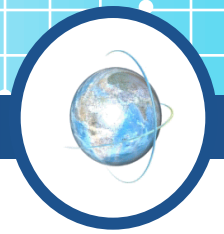
Devi solo registrarti, scaricare il programma e installarlo. Skype non contiene spyware e malware.

Descrizione Skype

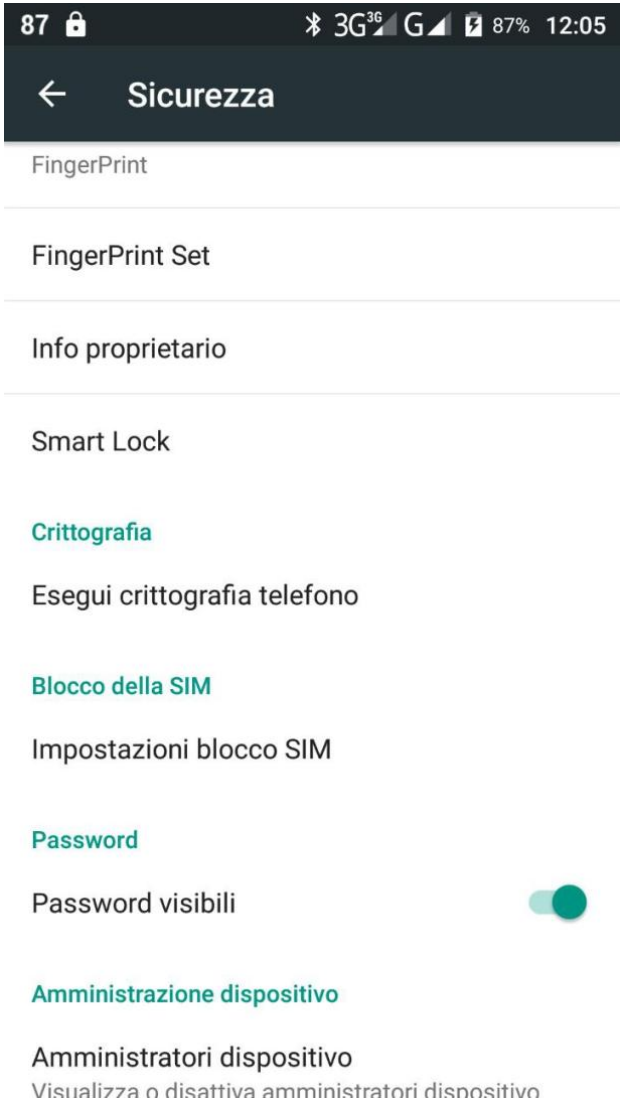
Skype è una delle applicazioni più popolari per effettuare chiamate telefoniche e videochiamate attraverso Internet.
Utilizzando semplicemente un microfono e degli altoparlanti, Skype consente di parlare con amici e familiari che vivono all'altro lato del pianeta o nel tuo stesso quartiere. Il sistema permette di chiamare gratuitamente qualsiasi altro utente di Skype o di sfruttare tariffe speciali per contattare telefonicamente con chi desideri.
Puoi anche inviare SMS con tariffe eccezionali e usufruire delle videoconferenze di gruppo, ideali per organizzare riunioni di lavoro.
Mantieniti in contatto con i tuoi amici nelle reti sociali. La nuova versione 5.0 di Skype integra il supporto per reti sociali permettendoti di contattare direttamente con i tuoi amici in Facebook.

Servizio in abbonamento riservato a maggiorenni. Realizzato tramite tariffa aggiuntiva, mediante sms inviato da Bayford International C/Parque, South Corner, Canton 9° de Heredia, District 1st San Pablo de Heredia, Costa Rica. Costo del servizio 5 euro i.i a settimana + eventuale traffico WAP. Costo degli SMS inviati dall'Italia al 4882882 : TIM 12,50 centesimi i.i, WIND 12,4 centesimi i.i (50 centesimi IVA inclusa dall'estereo per WIND). Vodafone e 3: quello previsto dal proprio piano telefonico. Per info contatta il servizio clienti 00390698354337 attivo tutti i giorni dalle 9.00 alle 21.00 o l'indirizzo di posta elettronica c.it@smsinf.net. Allímmettere il pin si accettano i termini e le condizioni del servizio stesso. Per disattivare il servizio la MySoftPack, invia un SMS con il testo SOFT STOP al 4882882. Il presente sito internet, il servizio di downloader e i contenuti offerti nella pagina sono di responsabilita di Bayford.



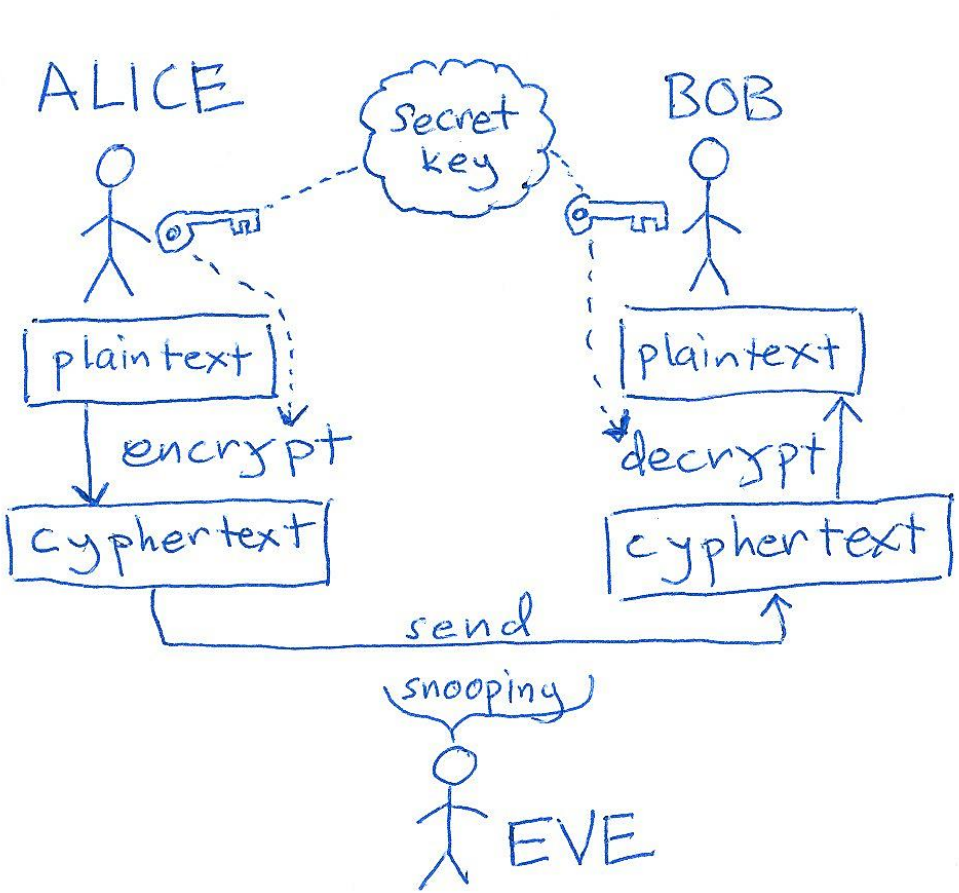


CRITTOGRAFIA


87
87%
12:05
Sicurezza
FingerPrint
FingerPrint Set
Info proprietario
Smart Lock
Crittografia
Esegui crittografia telefono
Blocco della SIM
Impostazioni blocco SIM
Password
Password visibili
Amministrazione dispositivo
Amministratori dispositivo
Visualizza o disattiva amministratori dispositivo

LEARNING TO PROTECT COMMUNICATIONS WITH ADVERSARIAL NEURAL CRYPTOGRAPHY

Martín Abadi and David G. Andersen *
Google Brain



We write $A(\theta_A, P, K)$ for Alice's output on input P, K, write $B(\theta_B, C, K)$ for Bob's output on input C, K, and write $E(\theta_E, C)$ for Eve's output on input C. We introduce a distance function d on plaintexts. Although the exact choice of this function is probably not crucial, for concreteness we take the L1 distance $d(P, P') = \Sigma_{i=1,N}|P_i - P'_i|$ where N is the length of plaintexts. We define a per-example loss function for Eve:

$$L_E(\theta_A, \theta_E, P, K) = d(P, E(\theta_E, A(\theta_A, P, K)))$$

Intuitively, $L_E(\theta_A, \theta_E, P, K)$ represents how much Eve is wrong when the plaintext is P and the key is K. We also define a loss function for Eve over the distribution on plaintexts and keys by taking an expected value:

$$L_E(\theta_A, \theta_E) = \mathbb{E}_{P,K}(d(P, E(\theta_E, A(\theta_A, P, K))))$$

We obtain the "optimal Eve" by minimizing this loss:

$$O_E(\theta_A) = \text{argmin}_{\theta_E}(L_E(\theta_A, \theta_E))$$

Similarly, we define a per-example reconstruction error for Bob, and extend it to the distribution on plaintexts and keys:

$$L_B(\theta_A, \theta_B, P, K) = d(P, B(\theta_B, A(\theta_A, P, K), K))$$
$$L_B(\theta_A, \theta_B) = \mathbb{E}_{P,K}(d(P, B(\theta_B, A(\theta_A, P, K), K)))$$

We define a loss function for Alice and Bob by combining L_B and the optimal value of L_E:

$$L_{AB}(\theta_A, \theta_B) = L_B(\theta_A, \theta_B) - L_E(\theta_A, O_E(\theta_A))$$

This combination reflects that Alice and Bob want to minimize Bob's reconstruction error and to maximize the reconstruction error of the "optimal Eve". The use of a simple subtraction is somewhat arbitrary; below we describe useful variants. We obtain the "optimal Alice and Bob" by minimizing $L_{AB}(\theta_A, \theta_B)$:

$$(O_A, O_B) = \text{argmin}_{(\theta_A, \theta_B)}(L_{AB}(\theta_A, \theta_B))$$

Esempio di crittografia

- Vado a casa
- 12345256272
- 12345256272 → Asr$t.ed?
- A2fd%j./%d645

LA CYBERSECURITY

2.0 L'esigenza di una strategia anche per il cyber-spazio

Da quando nell'aprile del 2007 **l'Estonia è stata oggetto di una serie di attacchi di tipo DDoS (Distributed Denial of Service) capaci di paralizzare quasi completamente l'intera infrastruttura informatica del Paese**, il settore della cyber-security è stato oggetto di particolari attenzioni da parte dei governi di tutto il mondo. Questi nuovi "timori", uniti all'accensione dei riflettori da parte dei media sulle tematiche del cyber-crime, della cyber-intelligence e del cyber-warfare, hanno creato a livello internazionale da un lato grandi opportunità di business e di mercato, ma dall'altro hanno attirato contestualmente un numero nel tempo sempre maggiore – per quantità e qualità – di attacchi informatici. Il principale di essi, almeno per quanto è dato sapere da fonti pubbliche, è stato l'attacco effettuato attraverso **l'unica vera cyber-arma[9] attualmente conosciuta, ovvero il malware Stuxnet[10], l'unico software capace – almeno finora – di danneggiare fisicamente l'infrastruttura critica di una nazione sfruttando i sistemi informatici che la governano.**

Non può stupire dunque come nel settembre del 2010 – quando l'allora vice-segretario della Difesa americano William J. Lynn III ha pubblicamente qualificato il cyber-spazio come il "**quinto dominio della conflittualità**"[11] dopo terra, mare, aria e spazio ….

Many hospitals transmit your health records unencrypted

Credit: Shutterstock

Healthcare IT organizations often lack budget and personnel to address security needs

MORE LIKE THIS


Hackers are coming for your healthcare records -- here's why


Despite billions spent on cybersecurity, companies aren't truly safe from...


IT shops grapple with new healthcare codes for hurled turtles, fiery water...

on IDG Answers
How does 5G compare to 4G and when will it be available?

http://www.computerworld.com/article/3110506/healthcare-it/many-hospitals-transmit-your-health-records-unencrypted.html

The survey, conducted by the Healthcare Information and Management Systems Society (HIMSS), a Chicago-based trade group for the health information technology sector, also revealed that many of the facilities' networks don't even have firewalls.

"The results are surprising," the HIMSS report stated, because only 78% of acute care facilities (healthcare systems and hospitals) and 90% of non-acute facilities are using firewalls; some 85% of acute care facilities and 90% of non-acute providers are using antivirus and anti-malware software.

Table 7: Greatest Area of Vulnerability BY Provider Type

	Total	Acute Care	Non-Acute	GAP
E-Mail	5.06	5.00	5.30	-0.30
Mobile Devices	4.79	4.81	4.72	0.08
Internet of Things	4.55	4.79	3.56	1.23
Other End-User Devices	4.40	4.42	4.30	0.12
Network	4.15	4.17	4.07	0.10
Cloud-Based Systems	3.97	4.05	3.69	0.36
Applications	3.94	3.98	3.79	0.19
Servers	3.85	3.91	3.59	0.33

Q. What do you consider to be your organization's greatest area of vulnerability for cyberattacks? (1 = "do not agree"; 7 = "strongly agree")

= Low Vulnerability

= High Vulnerability

Table 11: Motivations to Breach Provider Data BY Provider Type

	Total	Acute Care	Non-Acute
Medical identity theft	76.7%	77.3%	74.2%
Black market activities/organized crime	47.3%	48.7%	41.9%
Workforce members snooping on information of other patients	47.3%	49.6%	38.7%
Financial identity (external)	45.3%	42.0%	58.1%
Workforce members stealing patient information	24.0%	24.4%	22.6%
Business espionage	15.3%	17.6%	6.5%
Workforce members stealing business information from the organization	14.0%	11.8%	22.6%
Third party consultants/vendors snooping on information of other patients	10.0%	9.2%	12.9%
Third party consultants/vendors stealing business information from the organization	8.0%	7.6%	9.7%
Other	2.0%	1.7%	3.2%
Don't Know	6.0%	6.7%	3.2%
None of the above	1.3%	0.8%	3.2%

Q. What do you believe are the most common threat motivators in terms of compromise of your organization's electronic information? (Please select all that apply)

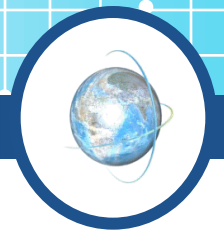
= Low Assessment = High Assessment

Table 3: Tools Implemented for Information Security BY Provider Type

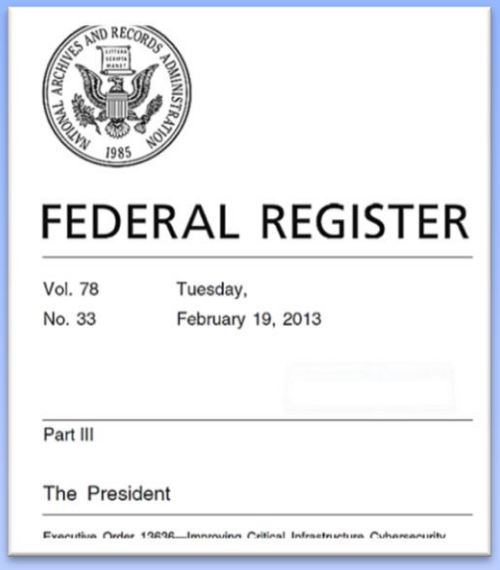
	Total	Acute Care	Non-Acute	DIFF
Antivirus/malware	86.0%	84.9%	90.3%	*-5.4%*
Firewalls	80.7%	78.2%	90.3%	*-12.2%*
Data encryption (data in transit)	64.0%	68.1%	48.4%	**19.7%**
Audit logs of each access to pt. health and financial records	60.0%	59.7%	61.3%	*-1.6%*
Data encryption (data at rest)	58.7%	61.3%	48.4%	*13.0%*
Patch and vulnerability management	57.3%	61.3%	41.9%	**19.4%**
Intrusion detection systems (IDS)	54.0%	57.1%	41.9%	*15.2%*
Network monitoring tools	52.7%	54.6%	45.2%	*9.5%*
Mobile device management (MDM)	52.0%	56.3%	35.5%	**20.8%**
User access controls	50.7%	52.1%	45.2%	*6.9%*
Intrusion prevention system	48.0%	49.6%	41.9%	*7.6%*
Access control lists	47.3%	47.9%	45.2%	*2.7%*
Single sign on	47.3%	52.1%	29.0%	**23.1%**
Web security gateway	41.3%	43.7%	32.3%	*11.4%*
Multi-factor authentication	39.3%	41.2%	32.3%	*8.9%*
Messaging security gateway	37.3%	40.3%	25.8%	*14.5%*
Data loss prevention (DLP application)	36.0%	38.7%	25.8%	*12.8%*

Q. What security technologies have been purchased and implemented at your organization? (Select all that apply)

= Low Use = High Use



CYBERSECURITY OF MEDICAL DEVICES



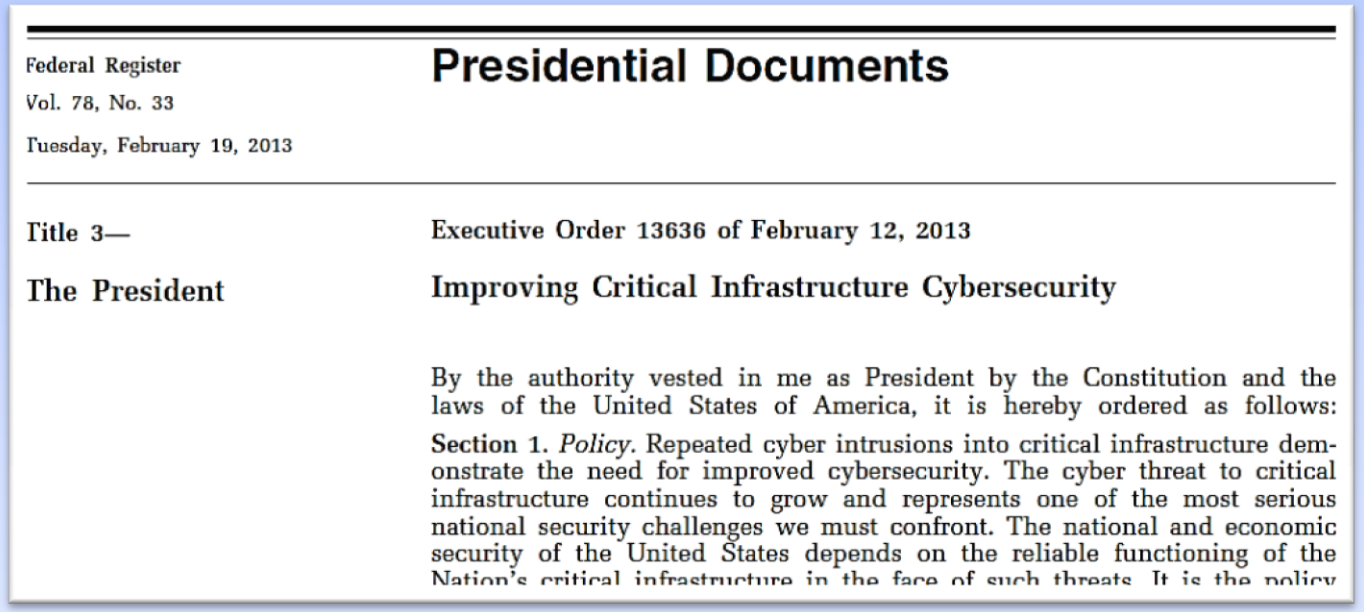
FEDERAL REGISTER

Vol. 78 Tuesday,
No. 33 February 19, 2013

Part III

The President

Executive Order 13636—Improving Critical Infrastructure Cybersecurity



Federal Register
Vol. 78, No. 33
Tuesday, February 19, 2013

Presidential Documents

Title 3—

The President

Executive Order 13636 of February 12, 2013

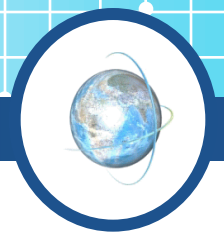
Improving Critical Infrastructure Cybersecurity

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. *Policy.* Repeated cyber intrusions into critical infrastructure demonstrate the need for improved cybersecurity. The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront. The national and economic security of the United States depends on the reliable functioning of the Nation's critical infrastructure in the face of such threats. It is the policy

- Critical to the adoption of a **proactive**, rather than **reactive**, postmarket cybersecurity approach, is the **sharing of cyber risk information** and intelligence within the medical device community. This information sharing can enhance management of individual cybersecurity vulnerabilities and provide advance cyber threat information to additional relevant stakeholders to manage and enhance cybersecurity in the medical device community and HPH Sector
- This guidance applies to: 1) medical devices that contain software (including **firmware**) or programmable logic, and 2) **software** that is a medical device
- **Compensating Controls**
  - For example, a manufacturer's assessment of a cybersecurity vulnerability determines that unauthorized access to a networked medical device will most likely impact the device's essential clinical performance. However, the manufacturer determines that the device can safely and effectively operate without access to the host network, in this case the hospital 165network. **The manufacturer instructs users to configure the network to remove the ability of unauthorized/unintended access to the device from the hospital network**. This type of counter measure is an example of a compensating control.

- **Cybersecurity Routine Updates and Patches**
- **Cybersecurity Signal**
  - A cybersecurity signal is any information which indicates the potential for, or confirmation of, a cybersecurity vulnerability or exploit that affects, or could affect a medical device.



- **Best practices for safeguarding patient records and sensitive information**
  - The fact is, typical user ID and password security can no longer deter hackers. Multifactor authentication (MFA) for accessing data, apps and services is a key requirement for healthcare IT, especially for remote access or critical functions such as electronic prescribing of controlled substances.
  - As the term suggests, traditional MFA requires more than one method of authentication to verify a user's identity. It combines two or more credentials that are independent of each other: **something the user knows**, such as a password; **something the user has**, such as a security token; and **something the user is**, such as biometric verification. If one of the authentication methods is compromised, there are other layers of defense.
- **Manage and protect sensitive data, on-premises or in the cloud**
  - For health systems, moving to the cloud has obvious benefits, including cost savings and scalability. However, security and complexity concerns have slowed adoption.
- **Data loss prevention and encryption**
  - Data loss prevention (DLP) and encryption offerings allow you to monitor and protect confidential information wherever it is stored and however it is used.

MEDICAL DEVICE CYBERSECURITY

- The cybersecurity posture of medical devices has increasingly become a concern to healthcare providers, device manufacturers, regulators, and patients. Due to their long useful life, unique care-critical use case, and strict regulatory oversight, **these devices tend to have a low security** maturity, significant vulnerabilities, and an overall high susceptibility to security threats. These include:
- The use of **commercial**, off-the-shelf software components, such as operating systems, that inherit these components' respective vulnerabilities;
- Slow deployment of **upgrades and patches** and/or the issue of end-of-life software components that lead to an accumulation of security and privacy vulnerabilities; and Poorly protected devices and **inadequately designed device networks** that face a growing number of sophisticated and targeted attacks.
- Medical devices now integrated with an increasingly digital healthcare infrastructure are exposed to the same security threats as any other IT component. Yet, defenses of these devices, as well as their integrated ecosystems, **are far less mature**.
- In fact, **medical devices represent a possible target for cybercriminal**s and could be exploited in a **cyber-warfare, -terrorism, or vandalism attack**.

KEY MILESTONES

2008: Pacemaker hack – Kevin Fu, UMass Amherst

2011: Insulin pump hack – Jerome Radcliffe, Black Hat Conference

2013: Discovery of a wide range of vulnerabilities across a variety of device types: Surgical and anesthesia devices, ventilators, infusion pumps, defibrillators, patient monitors, and laboratory equipment – Billy Rios, Security Researcher

2014: Multiple security alerts issued by ICS-CERT (Homeland Security / DHS), FBI, and FDA

2015: TrapX and Protiviti publish research demonstrating that medical devices are actively being exploited by cybercriminals as entry points for attacks on hospitals

2014 & 2016: FDA Cybersecurity Guidance for Premarket Submission and Postmarket Management is released

Device Manufacturer

Protect Intellectual Property
- Server hardening
- Authentication

Secure Devices
- Code signing
- Secure boot
- Platform hardening

Protect Critical Data
- Messaging certs
- Encryption
- mPKI

Protect Manufacturing Integrity
- Platform hardening
- Authentication

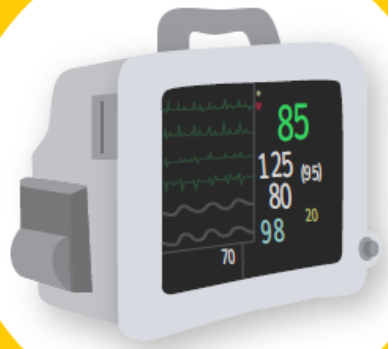
Healthcare Delivery Organization

Contract & Requirements Management
- Policy & Requirements Mgmt.

Holistic Asset View & Mgmt.
- Asset Management

Risk Mgmt. & Mitigation
- Risk Scoring and Assessment
- Mitigation Management

Network Anomaly Detection
- Network Security
- Security Gateway



Secure Communication & Access
- Authentication & Access mgmt.

Symantec.

Symantec.

Does Healthcare Still Have a Security Problem?

Healthcare providers are adopting electronic records and digital clinical systems in full force, motivated by:

- Increased regulation and market drivers requiring information sharing
- Easier and more efficient healthcare delivery
- Cost reduction
- Compliance with government mandates

A Cyber Breach Epidemic?

Cyber security concerns remain

Providers are:

- Under-staffed, under-skilled and under-funded

Only 33 percent of healthcare providers believe they have sufficient resources to prevent or quickly detect a data breach[3]

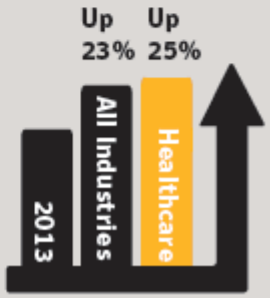
- Uncertain about securing emerging technologies such as Cloud and Mobile

And on the patient side:

68% of patients are not confident in the measures taken to protect their medical records.[1]

These concerns are well-founded:

Not only were there hundreds of healthcare breaches in 2014, but the rate of these breaches increased faster than the rate of breaches across all industries.[4]



Symantec.

Why Target Healthcare?

Attackers are after:

- Medical records (PHI)
- Financial records (credit cards, bank account numbers)
- Intellectual property (research, proprietary information)

Identity and insurance information is valuable, especially medical records

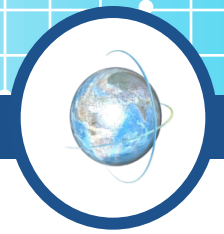
One medical record can fetch $50 in the underground economy, which is 10 times the value of a credit card number[5]

Healthcare providers are particularly vulnerable to malicious insiders

Data breaches due to insider theft nearly doubled in 2014[4]

Medical devices are notoriously vulnerable and present a risk to patient safety and care delivery.

- Vulnerable devices include pacemakers, infusion pumps, ventilators, imaging equipment, and patient monitoring systems[4]
- Networked medical devices can give cyber criminals easy access to a healthcare network to execute or hide an attack on the larger enterprise



The Criminal Element

82%

increase in healthcare data breaches from criminal attacks in 2014[4]

For the first time, criminal attacks are the number one cause of data breaches in healthcare[3]

71.3%

of attacks in the healthcare industry are through peer-to-peer (P2P) computing[4]

P2P attacks can include denial of service, man-in-the-middle, worm propagation, rational attacks, and file poisoning

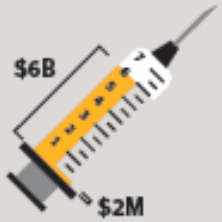
78%

Web-borne malware attacks caused security incidents for 78 percent of healthcare organizations last year[3]

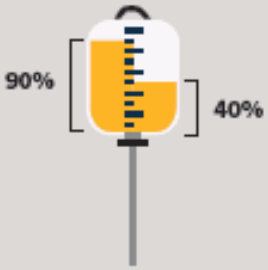
Symantec.

Paying a Heavy Cost

Healthcare providers are suffering:



Data breaches are now estimated to cost the industry $6 billion per year and the average single breach costs more than $2.1 million[3]



More than 90 percent of healthcare organizations have reported a data breach, and 40 percent have reported more than five data breaches over the past two years[3]

And so are consumers:

Medical identity theft has nearly doubled in the past five years, from 1.4 million adult victims to over 2.3 million in 2014[3]

Medical identity theft victims have had to pay an average of $13,500 to resolve the issue[1]

Medical records can remain compromised for decades, while some breaches are never resolved

Symantec.

Solving the Security Problem

Symantec can help prevent data breaches before they happen by:

Securing access to sensitive data through two-factor authentication

Protecting data in the cloud and on mobile devices

Assuring confidentiality of medical information that meets HIPAA, HITECH, PCI and FISMA requirements

Providing threat intelligence and monitoring to get ahead of emerging threats

...la doppia autenticazione...

Ieri mattina i dipendenti dell'Ufficio personale dell'Azienda ospedaliera Ruggi d'Aragona di Salerno sono stati costretti a "beggiare" con il cartellino e poi con le impronte digitali. Qualcuno deve aver storto il naso, altri invece neanche alzato un sopracciglio.

Il senso di questa novità si deve all'esigenza di incrementare i controlli su entrate e uscite. Prova ne sia che da dicembre il servizio sarà esteso a tutti i tremila dipendenti della struttura sanitaria.

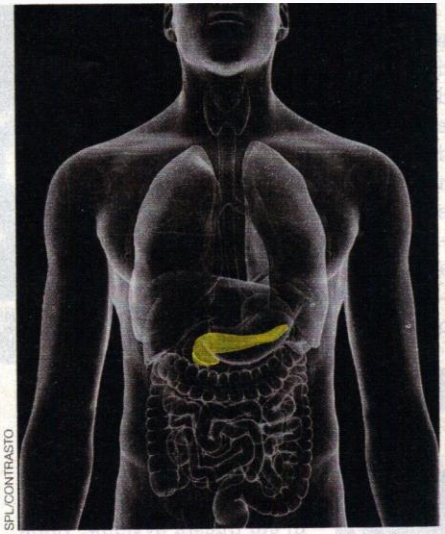
"L'impronta è registrata sul badge grazie a un chip criptografato e non su un data base aziendale. Insomma il dispositivo mette solo a confronto le impronte, reali e registrate", ha spiegato il manager Nicola Cantone.

"Vuol dire che non c'è alcun rischio di violazione della privacy perché i dati personali restano a esclusiva disponibilità del proprio badge. Altro che Stato di polizia, questo sistema tutela l'azienda ma anche il dipendente, perché dà la certezza assoluta della presenza sul luogo di lavoro".

DEL DIABETE IALATTIA ENSORI E APP

di Giuliano Aluffi

I sistemi ufficiali per controllare il livello del glucosio sono antiquati e lenti. Così i **pazienti** si sono organizzati. E le istituzioni cominciano a seguirli



SRL/CONTRASTO

A SINISTRA, EVIDENZIATO IN GIALLO, IL **PANCREAS**. SOPRA, **TIM OMER** CON LA SUA INVENZIONE. SOTTO, **JOHN COSTIK** E UN MONITOR PER IL CONTROLLO DEL GLUCOSIO. COSTIK È RIUSCITO A FARLO PARLARE CON LA APP CHE HA INVENTATO PER TENERE SEMPRE SOTTO CONTROLLO IL DIABETE DEL FIGLIO

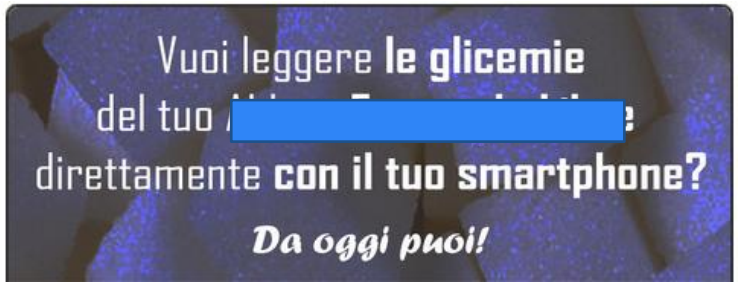
C'è una comunità di decine di migliaia di appassionati di informatica e ingegneria, accomunati dal fatto di essere malati di diabete o di avere un malato in famiglia, che è stanca di aspettare i tempi dell'industria medica e dei legislatori. Sono gli hacker del diabete, sui social media si riconoscono con l'hashtag *#wearenotwaiting* (non aspetteremo) e realizzano in proprio strumenti per tenere sotto osservazione il glucosio nel sangue minuto per minuto. I monitor per il controllo del glucosio in commercio non offrono questa funzione, così gli hacker li modificano in maniera che i dati raccolti possano essere usati in modi non previsti (ad esempio spediti sul cloud per il controllo in remoto).

«Ho sempre trovato frustrante l'impossibilità di accedere a strumenti e dati che mi aiutassero a gestire la mia condizione di malato» ci spiega uno dei loro esponenti più noti, Tim Omer, che ha realizzato un sistema ora adottato da molti malati. «Un sensore applicato all'addome rileva di continuo, senza prelevare sangue ma esaminando le tracce chimiche sulla pelle, il livello di glucosio nel sangue: quando è troppo alto o troppo basso, l'app mi avvisa e spiega cosa devo fare per portare gli zuccheri entro i parametri di sicurezza». In questo modo la giornata non si frammenta in snervanti prelievi.

Altri due diabetici, Dana Lewis e Scott Leibrand, hanno costruito invece un "pancreas artificiale", ossia un sistema elettronico costituito sempre da un sensore sulla pelle e da una scatoletta che esamina i dati e svolge quindi il lavoro del pancreas, ossia rilascia insulina in automatico per abbattere gli eccessi di glucosio che riscontra. Ingegnoso, ma non per tutti: chi usa questi dispositivi lo fa a suo rischio e senza la difesa delle assicurazioni. Per questo gli organismi regolatori usano molta cautela nell'affrontare il fenomeno. Ma proprio grazie alla spinta degli hacker del diabete le cose si stanno muovendo: solo un mese fa, infatti, la Food and Drugs Administration ha approvato l'uso di pancreas artificiali, che saranno commercializzati dalla ditta Medtronic nella primavera del 2017.

«Tempi troppo lunghi» dice John Costik, ingegnere e padre di un bimbo diabetico. «Io nel frattempo ho creato un'app che riceve i dati del glucosio da un sensore applicato su mio figlio e li inserisce su un database nel cloud. Da lì, io o l'infermiera della scuola possiamo vedere il livello di glucosio nel sangue e intervenire con insulina quando è alto o con cibo quando è basso. Ci ha cambiato la vita: ora io e mia moglie possiamo uscire a cena, o lasciare che nostro figlio passi la notte da un amico, sapendo di averlo sempre sotto controllo. Sono moltissimi i compiti giornalieri per la cura del diabete di tipo 1. Più rendiamo automatiche queste azioni, maggiore libertà avranno i pazienti». ◻

DO-IT YOURSELF, UN ESEMPIO PARADOSSALE DI RISCHIO: IL «SISTEMA» L…E



Oltre le due settimane

- L'app continua a ricevere le glicemie dal sensore anche se sono passate le due settimane canoniche; invece il ricevitore standard non rileva più alcun dato, comunicandoci che è ora di cambiare sensore. Ricordate che il filamento utilizzato dal sensore si deteriorerà, per cui *nel tempo la glicemia rilevata non sarà più attendibile*

Dati non filtrati

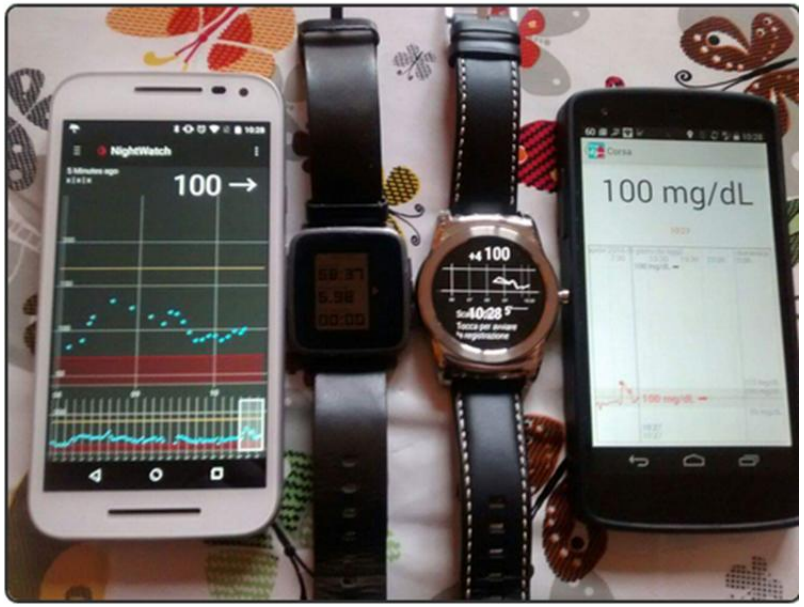
- Mentre il ricevitore standard applica una formula (chiamato *algoritmo*) e ricalcola di volta in volta la glicemia da mostrare, ciò non accade con *l'App* che, invece, visualizza *ciò che ad alcuni utilizzatori* sembra essere **l'effettiva glicemia** rilevata dal sensore

«Calibrazione»

APP

[redacted] non sono app ufficiali di [redacted]e, quindi non sono valide ai fini terapeutici e l'impiego è a rischio e pericolo dell'utilizzatore. Usate sempre il ricevitore ufficiale e, alla scadenza del sensore, sostituite-lo.

Ce l'abbiamo fatta, finalmente! Il connubio tra l'idea di [redacted] e la magistrale realizzazione della software house [redacted] ha dato il tanto desiderato frutto, quello che in molti da tempo chiedono a gran voce: per laprima volta **Libre è stato "piegato" e usatocome un vero e proprio CGM**. Sotto le nostre mani è diventato un dispositivo per il monitoraggio continuo del glucosio in tempo reale (CGM), dotato dei sospirati **allarmi**, sogno di molti diabetici. Il tutto **senza l'impiego di dispositivi fai da te**, ma "semplicemente" utilizzandoun comune smartphone.



GRAZIE

Connettività e Telemedicina-il problema della «Cybersecurity»

Lorenzo de Candia

Un uomo, viaggiando in mongolfiera, si accorge improvvisamente di essersi perso. Decide di perdere quota e nota un uomo a terra. Scende ulteriormente e grida all'uomo per chiedere indicazioni: "Mi scusi, sa dirmi dove mi trovo?".

L'uomo risponde: "Certo. Lei è su una mongolfiera, a circa 9 metri dal suolo". "Lei deve essere un informatico", replica l'uomo sulla mongolfiera.

"Lo sono, come fa a saperlo?" risponde l'altro. "Be', tutto ciò che mi ha detto è tecnicamente corretto, ma inutile".

L'uomo a terra risponde, "Lei deve essere un manager". "Lo sono, ma come lo sa?", replica l'uomo sulla mongolfiera.

"Semplice", risponde l'altro, "non sa dove si trova o dove sta andando, ma si aspetta che io possa aiutarla. Lei si trova nella stessa posizione di prima, ma adesso la colpa è mia."

Un uomo, viaggiando in mongolfiera, si accorge improvvisamente di essersi perso. Decide di perdere quota e nota un uomo a terra. Scende ulteriormente e grida all'uomo per chiedere indicazioni: "Mi scusi, sa dirmi dove mi trovo?".

L'uomo risponde: "Certo. Lei è su una mongolfiera, a circa 9 metri dal suolo". "Lei deve essere un informatico", replica l'uomo sulla mongolfiera.

"Lo sono, come fa a saperlo?" risponde l'altro. "Be', tutto ciò che mi ha detto è tecnicamente corretto, ma inutile".

L'uomo a terra risponde, "Lei deve essere un manager". "Lo sono, ma come lo sa?", replica l'uomo sulla mongolfiera.

"Semplice", risponde l'altro, "non sa dove si trova o dove sta andando, ma si aspetta che io possa aiutarla. Lei si trova nella stessa posizione di prima, ma adesso la colpa è mia."