X Conferenza Nazionale sui Dispositivi Medici
18 / 19 DICEMBRE 2017 ROMA
AUDITORIUM ANTONIANUM - VIALE MANZONI, 1

Cybersecurity e dispositivi medici:

Privacy e sicurezza della salute, due facce della stessa medaglia

Ing. Maurizio Rizzetto – Gruppo di lavoro ICT
AIIC Associazione Italiana Ingegneri Clinici

Global and local impact Systems and Device

- Volume of technology ↑
- Devices' embedded intelligence ↑
- Devices' integration ↑
- Locus of care expanding

Rif. Yadin David BAC

FDA warns of security flaw in Hospira infusion pumps

31 luglio 2015

finance.yahoo.com

July 31 04:11 PM

BOSTON, July 31 (Reuters) - The U.S. Food and Drug Administration on Friday advised hospitals to stop using Hospira Inc's Symbiq infusion system, saying a security vulnerability could allow cyber attackers to take control of the system remotely.

The agency issued the advisory some 10 days after the U.S. Department of Homeland Security warned of the vulnerability in the pump, which is used to deliver medications directly into the bloodstream of patients.

The FDA and DHS cited research from independent cyber security expert Billy Rios, who found that remote attacks could be launched on patients by accessing a hospital's network.

Both government agencies said they know of no cases where such an attack has been launched, but the FDA said in its advisory that it strongly encouraged healthcare facilities to stop using the Symbiq infusion pump system and move to other devices.

"This (vulnerability) could allow an unauthorized user to control the device and change the dosage the pump delivers, which could lead to over- or under-infusion of critical patient therapies," the agency said in its warning.

The warning came as industry and government regulators are placing unprecedented attention on public safety risks posed by cyber vulnerabilities in products with embedded computers.

U.S. FOOD & DRUG ADMINISTRATION

A to Z Index | Follow FDA | En Español

Search FDA

Home | Food | Drugs | Medical Devices | Radiation-Emitting Products | Vaccines, Blood & Biologics | Animal & Veterinary | Cosmetics | Tobacco Products

Medical Devices

Home > Medical Devices > Medical Device Safety > Safety Communications

Safety Communications

2017 Safety Communications

2016 Safety Communications

Firmware Update to Address Cybersecurity Vulnerabilities Identified in Abbott's (formerly St. Jude Medical's) Implantable Cardiac Pacemakers: FDA Safety Communication

SHARE TWEET LINKEDIN PIN IT EMAIL PRINT

Date Issued

August 29, 2017

Audience

- Patients with a radio frequency (RF)-enabled St. Jude Medical implantable pacemaker
- Caregivers of patients with an RF-enabled St. Jude Medical implantable cardiac pacemaker
- Cardiologists, electrophysiologists, cardiothoracic surgeons, and primary care physicians treating patients with heart failure or heart rhythm problems using an RF-enabled St. Jude Medical implantable cardiac pacemaker

Medical Specialties

Cardiac Electrophysiology, Cardiology, Cardiothoracic Surgery, Heart Failure

Devices

Abbott's (formerly St. Jude Medical's) implantable cardiac pacemakers, including cardiac resynchronization therapy pacemaker (CRT-P) devices, provide pacing for slow or irregular heart rhythms. These devices are

Purpose

On August 23, 2017, the FDA approved a firmware update that is now available and is intended as a recall, specifically a corrective action, to reduce the risk of patient harm due to potential exploitation of cybersecurity vulnerabilities for certain Abbott (formerly St. Jude Medical) pacemakers. "

FDA to recall 745,000 pacemakers vulnerable to Cyber Attack

Posted By **Naveen Goud** 29 agosto 2017

49

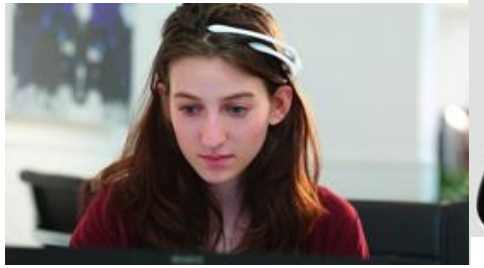
The Food and Drug Administration (FDA) of United States has issued an alert this week for a voluntary recall of approximately 745,000 pacemakers made by St Jude Medical, now owned by US Manufacturer Abbott.

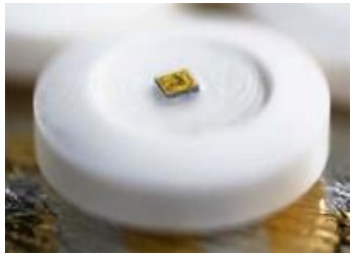
And as per the data available with the FDA, more than 465,000 of the pacemakers are implanted in US patients and another 280,000 are being used worldwide.

Top 10 Health Technology Hazards for 2018 ECRI Institute

1. Ransomware and Other Cybersecurity Threats to Healthcare Delivery Can Endanger Patients
2. Endoscope Reprocessing Failures Continue to Expose Patients to Infection Risk
3. Mattresses and Covers May Be Infected by Body Fluids and Microbiological Contaminants
4. Missed Alarms May Result from Inappropriately Con gured Secondary Noti cation Devices and Systems
5. Improper Cleaning May Cause Device Malfunctions, Equipment Failures, and Potential for Patient Injury
6. Unholstered Electrosurgical Active Electrodes Can Lead to Patient Burns
7. Inadequate Use of Digital Imaging Tools May Lead to Unnecessary Radiation Exposure
8. Workarounds Can Negate the Safety Advantages of Bar-Coded Medication Administration Systems
9. Flaws in Medical Device Networking Can Lead to Delayed or Inappropriate Care
10. Slow Adoption of Safer Enteral Feeding Connectors Leaves Patients at Risk

BIOSENSING WEARABLES LANDSCAPE





COMMODITY ZONE

GROWING LONG TAIL

MOVEMENT	HEART RATE	SLEEP	TEMPERATURE	RESPIRATION	SKIN CONDUCTANCE	BRAIN ACTIVITY	HYDRATION	POSTURE	GLUCOSE	OXYGEN LEVEL	HEART RATE VARIABILITY	MUSCLE ACTIVITY	BLOOD PRESSURE	EYE-TRACKING	INGESTION
amiigo	amiigo	amiigo	BASIS	ATHOS	BASIS	EMOTIV	corventis	JINS MEME	dexcom	iHealth	corventis	ATHOS	iHealth	JINS MEME	proteus
BASIS	ATHOS	BASIS	BODYMEDIA	corventis	BODYMEDIA	mc10	electrozyme	LUMO	GLYSENS INCORPORATED	OWLET	Zephyr	electrozyme			
BODYMEDIA	BASIS	BODYMEDIA	Empatica	Perminova	Empatica	Multimon	mc10	Zephyr	Google	Withings					
corventis	corventis	fitbit	ATHOS	SPIRE	NeuMitra	NeuroSky	Perminova								
Empatica	Empatica	GARMIN	corventis	Zephyr											
fitbit	fitbit	iHealth	mc10												
GARMIN	GARMIN	JAWBONE	OWLET												
iHealth	iHealth	LUMO	Sproutling												
JAWBONE	iRhythm	MISFIT	Tempdrop												
JINS MEME	mc10	NeuMitra													
kiwi	OWLET	OWLET													
LUMO	Perminova	Perminova													
mc10	proteus	proteus													
MISFIT	SAMSUNG	SAMSUNG													
NeuMitra	senSoria	striiv													
OWLET	striiv	watermark													
proteus	Withings	Withings													
striiv	Zephyr	Zephyr													
SAMSUNG															
senSoria															
SPIRE															
Sproutling															
Withings															
Zephyr															

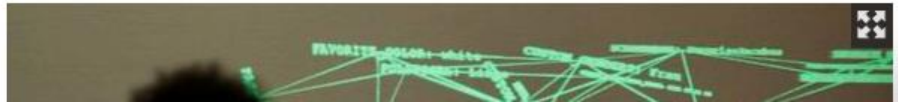
Source: Rock Health review of 75+ companies (companies are selected, not comprehensive)

DDOS

Il cyber attacco contro Internet negli Usa partito dalle case «intelligenti»

L'attacco è arrivato da oggetti «smart»: videoregistratori, frigoriferi, telecamere di sicurezza, router e sistemi per il controllo dei neonati. Wikileaks rivendica

di FEDERICO CELLA ★ 32



3 243 7

DIGITAL DAY DDAY.it #OLED #TV #MACBOOK PRO #HUAWEI MATE 9

NEWS TEST E PROVE INCHIESTE E REPORTAGE GUIDE PRODOTTI FORUM

C'è l'Internet of Things alla base dell'attacco che ha piegato il Web

di Emanuele Villa - *22/10/2016 18:43* 3

POWERED BY NTT DATA

Cyber Security *Cybersecurity*

Le botnet IoT infettate da Mirai attaccano ancora. Stavolta il bersaglio è una nazione

Il prossimo bersaglio dei computer zombie che hanno attaccato il provider Dyn potrebbe essere un paese europeo a meno che non impariamo a proteggere la nostra Internet of Things

Arturo Di Corinto 4 novembre 2016

Le **botnet** controllate dal malware **Mirai** stanno attaccando di nuovo. E come avevamo scritto sulla base dell'allarme di Bruce Schneier, il bersaglio stavolta potrebbe essere un'intera nazione.

Questa è almeno la tesi di **Kevin Beaumont**, ricercatore in **cybersecurity**, che, notando un insolito volume di traffico verso la **Liberia**, ha potuto osservare una serie

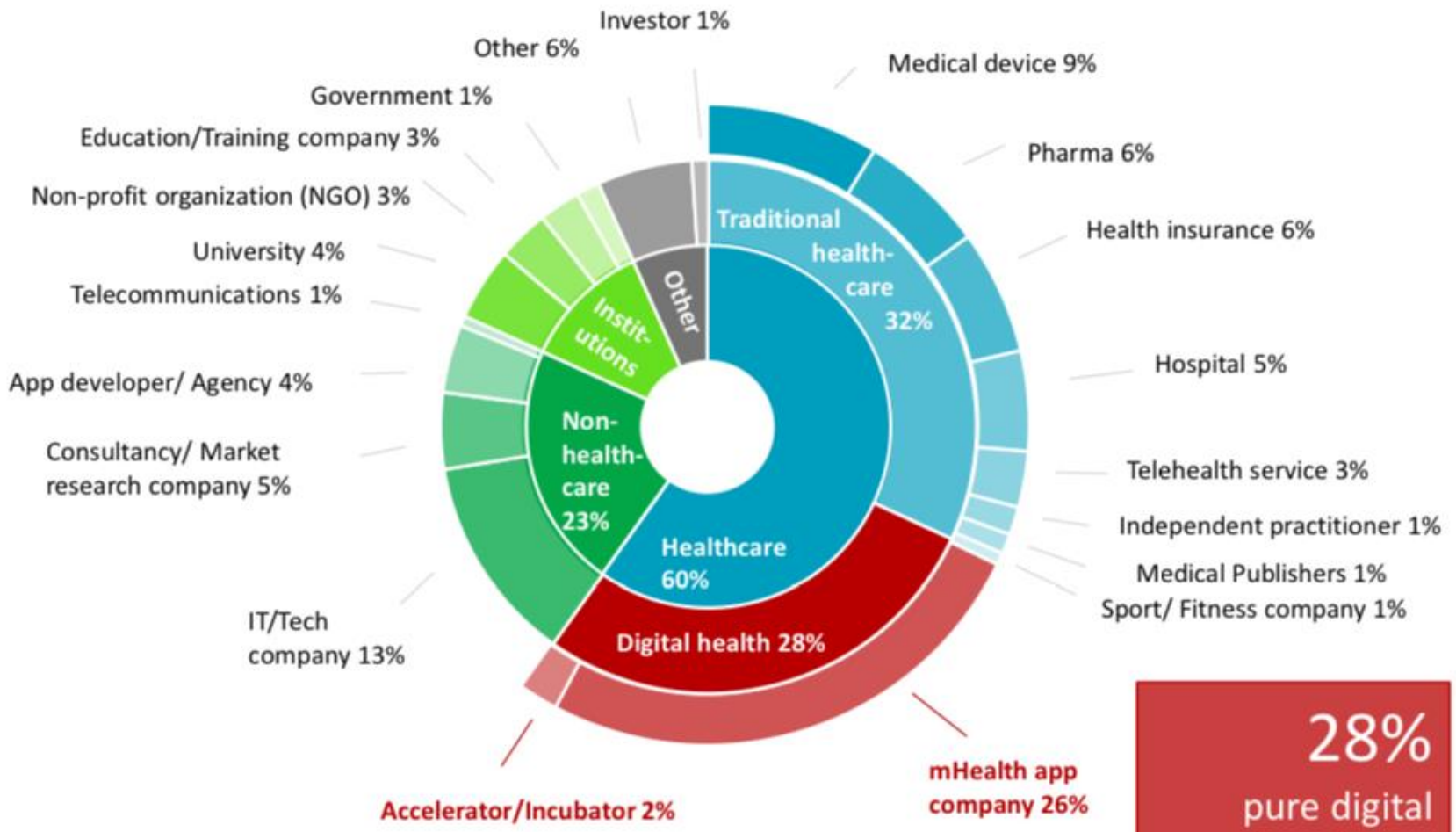
325,000 mHEALTH APPS AVAILABLE – GOOGLE PLAY STORE IS NOW NUMBER ONE FOR HEALTHCARE APPS, OVERTAKING APPLE APP STORE

Number of mHealth apps displayed in App Stores

Source: Research2Guidance - mHealth App Developer Economics study 2017 - n = 2,400

DIGITAL INTRUDERS: THE HEALTHCARE MARKET IS SHAKEN UP BY NEW, PURELY DIGITAL MARKET PLAYERS

Your organization is best described as:



28%
pure digital market players

Source: Research2Guidance - mHealth App Developer Economics study 2017 - n = 2,400

©Research2Guidance 2017

TIME

DIET & FITNESS

Bad News About Your Favorite Health Apps: They Don't Work

By Alexandra Sifferlin @acsifferlin | Oct. 31, 2013

Share Like 462 Tweet G+1 7 Share 29 Pin it Read Later

They promise a lot — from helping you to burn "fuel" to shedding pounds, but when it comes to making a difference in your health, these apps mostly fall short.

Getty Images

Search the Apple iTunes app store for "health" and you'll find more than 43,000 apps that work on weight loss or fitness, such as Calorie Counter, FitBit and Nike Fuelband, or those run by Walgreens or WebMD that address more general health questions and problems. And there is a high demand for them, with an estimated 660 million downloads for apps in this category as of June 2013.

But how well are they accomplishing what they claim to do? Are they helping users to lose weight, control their blood pressure, or sleep better? In a report by the IMS Institute for Healthcare Informatics, researchers evaluated all of the health care apps on how well they functioned and displayed relevant health information, to whether they provided helpful and potentially motivating reminders for good health habits. The researchers also interviewed physicians and the app providers about how useful the metrics were.

RELATED

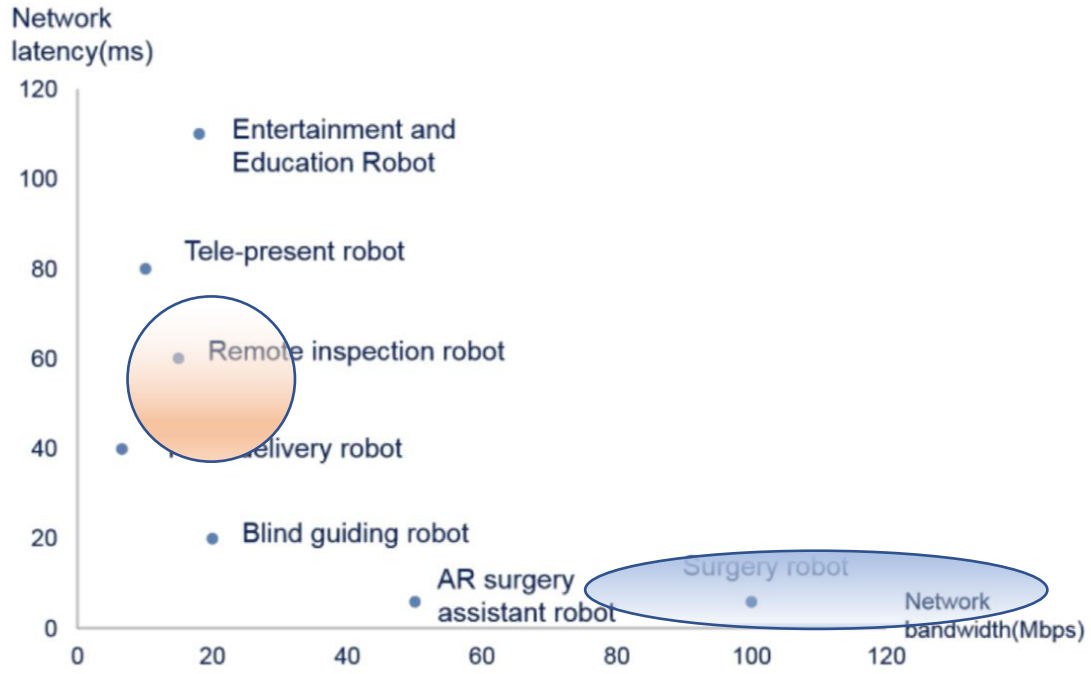
FDA To Regulate Health Apps

5 Great Health Apps You Should Download Now

In the Candy Store of iPhone Apps, Users Treat Health Apps Like Broccoli

RETI DATI - Banda di trasmissione

- 5G prossima generazione di comunicazione del Mobile attesa in fase di maturita per la fine del decennio attuale. Garantirà prestazioni teoriche di picco di 10 Gb/s e meno di 1 ms di ritardo



Network requirements for cloud robot applications [Source: Huawei X Labs]

Intelligenza artificiale – Precision Medicine

1. Big data analysis – analisi di grandi volumi di dati per estrarre nuove informazioni
2. Machine learning – Apprendimento automatico - fornisce ai computer l'abilità di apprendere senza essere stati esplicitamente programmati.
3. Artificial neural networks – rete neurale artificiale - modelli matematici che consentono ad una macchina di ricavare informazioni da dati non strutturati complessi come ad esempio da immagini mediche.

Malware vs Dispositivo Medico

La presenza di malware può causare interruzione di servizio sanitario

- I malware si propagano attraverso le apparecchiature collegate in rete (anche MD) provocando malfunzionamento degli assets IT (disabilitazione degli accessi, criptazione dei dati ecc).
- In un contesto sanitario un attacco da parte di malware può avere un impatto sull'erogazione di servizi a causa di:
  - Inaccessibilità ai dati dei pazienti
  - Mancanza di funzionalità di dispositivi medici collegati alla rete
  - Disabilitazione di servizi di terze parti
  - Interruzione servizi di approvvigionamento di farmaci e presidi medici
  - Malfunzionamenti di servizi infrastrutturali
- Tali interruzioni possono portare alla cancellazione di procedure mediche e/o alterazioni del workflow (per esempio per passaggio a procedure cartacee di emergenza), al danneggiamento di dispositivi medici, alla diffusione involontaria di dati sensibili, alla chiusura di specifici servizi sanitari.
- ritardo/mancanza nell'erogazione di un servizio sanitario con un potenziale danno al paziente

Proposta - Fase di acquisizione DM in rete

- Valutazione del prodotto in fase d’acquisto
- Le Apparecchiature medicali che devono funzionare in rete devono rispondere a specifiche esigenze di sicurezza rispetto all’impatto sulla cybersecurity
- La fase di acquisizione richiede collaborazione multidisciplinare (CE/IT/responsabile sicurezza delle informazioni)
- Richiedere il MDS2 Form che evidenzia che caratteristiche di un dispositivo medico in rete rispetto alla sicurezza informatica (HIMSS vs 80001)

Manufacturer Disclosure Statement for Medical Device Security (MDS2)

Manufacturer Disclosure Statement for Medical Device Security – MDS²

SECTION 1

Device Category	Manufacturer	Document ID	Document Release Date

Device Model		Software Revision		Software Release Date	

Manufacturer or Representative Contact Information:	Company Name	Manufacturer Contact Information
	Representative Name/Position	

MANAGEMENT OF ELECTRONIC PROTECTED HEALTH INFORMATION (ePHI)	Yes No N/A	Note #
1. Can this device transmit or maintain electronic Protected Health Information (ePHI)?	_____	_____
2. Types of ePHI data elements that can be maintained by the device:		
a. Demographic (e.g., name, address, location, unique identification number)?	_____	_____
b. Medical record (e.g., medical record #, account #, test or treatment date, device identification number)?	_____	_____
c. Diagnostic/therapeutic (e.g., photo/radiograph, test results, or physiologic data with identifying characteristics)?	_____	_____
d. Open, unstructured text entered by device user/operator?	_____	_____
3. Maintaining ePHI - Can the device		
a. Maintain ePHI temporarily in volatile memory (i.e., until cleared on by power-off or reset)?	_____	_____
b. Store ePHI persistently on local media?	_____	_____
c. Import/export ePHI with other systems?	_____	_____
4. Mechanisms used for the transmitting, importing/exporting of ePHI – Can the device		
a. Display ePHI (e.g., video display)?	_____	_____
b. Generate hardcopy reports or images containing ePHI?	_____	_____
c. Retrieve ePHI from or record ePHI to removable media (e.g., disk, DVD, CD-ROM, tape, CF/SD card, memory stick)?	_____	_____
d. Transmit/receive or import/export ePHI via dedicated cable connection (e.g., IEEE 1073, serial port, USB, FireWire)?	_____	_____
e. Transmit/receive ePHI via a network connection (e.g., LAN, WAN, VPN, intranet, Internet)?	_____	_____
f. Transmit/receive ePHI via an integrated wireless connection (e.g. WiFi, Bluetooth, infrared)?	_____	_____
g. Other? _____	_____	

Proposta - Gestione dei DM in rete 1/2

- Sottoporre ai a scansioni di vulnerabilità anche i dispositivi medici connessi in rete al fine di identificare le vulnerabilità cyber– cosa non semplice da fare in sicurezza – serve un approccio diverso di quello utilizzato per gli assetts IT non medicali. Spesso gli assetts medicali non sono progettati per supportare questi scan.
- Migliorare la gestione del software medical device al fine di rispondere tempestivamente a problemi di sicurezza – non collegare alla rete se non serve – se ti attaccano te ne accorgi ? Dopo quanto?
- Gestire le perifiche esterne (es. USB) da utilizzi non necessari, gestire le credenziali d'accesso, aggiornamento del firmware (Hardening)
- Fare una revisione dei protocolli e procedure di sicurezza alla luce degli alerts/incidenti che vengono segnalati

Proposta - Gestione dei DM in rete 2/2

- Gestire i sistemi antivirus per i DM SW
- Adottare strategie per i DM che utilizzano ancora Windows XP – piano di sostituzione
- Utilizzare la normativa tecnica in vigore es. IEC 80001-1
- IC-IT collaborazione – in genere ognuno vede solo una parte del sistema (altri attori devono essere coinvolti: responsabili sicurezza, terze parti, ecc.)
- Gestire il rapporto con il fornitore/produttore del DM SW (es. accordi di responsabilità)
- Gestire i servizi sanitari basati su sistemi IT distribuiti sulla rete Internet e sviluppati da fornitori che non provengono dal mondo/mercato sanitario
- Coinvolgere alta direzione dell'organizzazione responsabile
- Supportare la formazione di nuove figure professionali nell'ambito della sicurezza sistema IT in generale

In This Section

ACCE/HIMSS Excellence in Clinical Engineering & IT Award

CHIME-HIMSS CIO of the Year Award

HIMSS-AMDIS Physician Executive Leader of the Year Award

ACCE/HIMSS Excellence in Clinical Engineering and Information Technology Synergies Award

The call for nominations are now closed. Award recipients will be announced in December 2017/January 2018. For more information, contact awards@himss.org

HIMSS 2017 Recipient

HIMSS ITALIAN COMMUNITY

Get involved on a regional level

HIMSS ITALIAN COMMUNITY

Benvenuti

Attraverso le attività della HIMSS Italian Community, HIMSS Europe desidera promuovere l´uso e l´adozione di tecnologie dell´informazione e della comunicazione nel settore sanitario italiano. Per questo motivo, HIMSS Europe si impegna a organizzare sessioni informative e formative per favorire lo scambio di conoscenze e creare opportunità esclusive di networking.

HIMSS Italia

La HIMSS Italian Community è composta dai professionisti italiani della salute e dell´ICT che lavorano nel settore sanitario pubblico e privato. La missione della HIMSS Italian Community è di creare una piattaforma di scambio per tutti coloro che ambiscono a fornire migliori servizi sanitari attraverso l´applicazione di soluzioni digitali. La Community permette ai suoi membri di:

- Accedere a un network nazionale e internazionale composto dai principali leader della salute digitale
- Rimanere costantemente aggiornati sulle più recenti innovazioni digitali nel campo della salute

Contact Us

Angela Velkova
Senior Communities Manager,
avelkova@himss.org
Office: +49 (0)30 34 65542 16
Mobile: +49 (0)172 871 85 31

Clemente Capasso
Business Development Manager
HIMSS Analytics
ccapasso@himss.org

Norme di riferimento

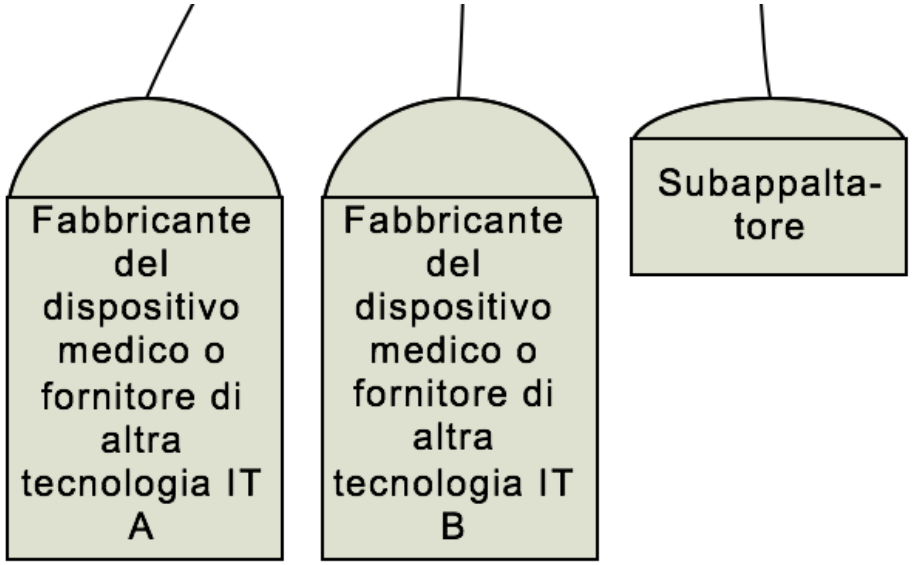
- CEI EN 60601 Apparecchi elettromedicali
- CEI EN 80001-1 – 2016 e famiglia – reti medicali con DM
- Regolamento DM 745/2017
- Regolamento Privacy 679/2016
- Linea Guida AGID sulla sicurezza
- Guida CEI 62-237/2015 gestione sw con scopo sanitario – Parte 1
- Guida CEI 62-252/2017 gestione sw con scopo sanitario – Parte 2
- AAMI TIR 57 Principles for medical device information security risk manag.
  - Come si applica la 14971 (risk manag MD) tenuto conto delle 80001
- Attesa per il 2019 - AAMI TIR 97 Principles for medical device information security – post market
- CEI UNI ISO IEC 20000-1 2012

CEI EN 80001-1 2016

- SICUREZZA (SAFETY) assenza di rischi inaccettabili di lesione fisica o di danni alla salute di persone/ cose/ ambiente
- SICUREZZA DEI DATI e DEL SISTEMA (SECURITY) risorse informatiche, dati e sistemi, sono ragionevolmente protette dal degrado della loro riservatezza, integrità e disponibilità
- EFFICACIA (capacità di produrre il risultato previsto per il paziente e per l'ORGANIZZAZIONE RESPONSABILE)

PROPRIETA CHIAVE

- SICUREZZA
- EFFICACIA
- SICUREZZA DEI DATI e DEL SISTEMA



80001 - xx

IEC TR 80001-2-1:2012	Application of risk management for IT-networks incorporating medical devices - Part 2-1: Step by step risk management of medical IT-networks - Pratical applications and examples
IEC TR 80001-2-2:2012	Application of risk management for IT-networks incorporating medical devices - Part 2-2: Guidance for the disclosure and communication of medical device security needs, risks and controls
IEC TR 80001-2-3:2012	Application of risk management for IT-networks incorporating medical devices - Part 2-3: Guidance for wireless networks
IEC TR 80001-2-4:2012	Application of risk management for IT-networks incorporating medical devices - Part 2-4: Application guidance - General implementation guidance for healthcare delivery organizations
IEC TR 80001-2-5:2014	Application of risk management for IT-networks incorporating medical devices - Part 2-5: Application guidance - Guidance on distributed alarm systems
ISO/TR 80001-2-6:2014	Application of risk management for IT-networks incorporating medical devices – Part 2-6: Application guidance – Guidance for responsibility agreements
ISO TR 80001-2-7:2015	Application of risk management for IT-networks incorporating medical devices -- Application guidance -- Part 2-7: Guidance for Healthcare Delivery Organizations (HDOs) on how to self-assess their conformance with IEC 80001-1
IEC TR 80001-2-8:2016	Application of risk management for IT-networks incorporating medical devices - Part 2-8: Application guidance - Guidance on standards for establishing the security capabilities identified in IEC TR 80001-2-2
IEC TR 80001-2-9:2017	Application of risk management for IT-networks incorporating medical devices - Part 2-9: Application guidance - Guidance for use of security assurance cases to demonstrate confidence in IEC TR 80001-2-2 security capabilities

Regolamento DM
Definizione dispositivo medico

«dispositivo medico»: qualunque strumento, apparecchio, apparecchiatura, software, impianto, reagente, ~~sostanza o altro prodotto~~ materiale o altro articolo, destinato dal fabbricante a essere impiegato sull'uomo, ~~utilizzato~~ da solo o in combinazione, ~~compreso il software destinato dal fabbricante ad essere impiegato specificatamente con finalità diagnostiche o terapeutiche e necessario al corretto funzionamento del dispositivo~~, per una o più delle seguenti destinazioni d'uso mediche specifiche:

- diagnosi, prevenzione, ~~controllo~~, monitoraggio, previsione, prognosi, ~~terapia~~ trattamento o attenuazione di ~~una~~ malattie~~a~~,
- diagnosi, ~~controllo~~ monitoraggio, ~~terapia~~ trattamento, attenuazione o compensazione di una ~~ferita~~ lesione o di una ~~handicap~~ disabilità,
- studio, sostituzione o modifica dell'anatomia oppure di un processo o stato fisiologico o patologico,
- ~~di intervento sul concepimento~~
- fornire informazioni attraverso l'esame *in vitro* di campioni provenienti dal corpo umano, inclusi sangue e tessuti donati,

e che ~~il quale prodotto~~ non esercita nel o sul corpo umano l'azione principale cui è destinato ~~con~~ mediante mezzi farmacologici~~, o~~ immunologici o ~~ne mediante processo~~ metabolici, ma la cui funzione ~~possa~~ può essere coadiuvata da tali mezzi.

Si considerano dispositivi medici anche i seguenti prodotti:

- dispositivi per il controllo del concepimento o il supporto al concepimento,
- i prodotti specificamente destinati alla pulizia, disinfezione o sterilizzazione dei dispositivi di cui all'articolo 1, paragrafo 4, e di quelli di cui al primo comma del presente punto;

allegato I - REQUISITI GENERALI DI SICUREZZA Capo II REQUISITI RELATIVI ALLA PROGETTAZIONE E ALLA FABBRICAZIONE

14 Fabbricazione dei dispositivi e interazione con il loro ambiente

14.2 I dispositivi sono progettati e fabbricati in modo tale da eliminare o ridurre per quanto possibile:

- d) i rischi associati alla possibile interazione negativa tra il software e l'ambiente tecnologico («ambiente IT») in cui opera e interagisce; Cybersecurity??? Sicurezza informatica ???

17 Sistemi elettronici programmabili — dispositivi contenenti sistemi elettronici programmabili e software che costituiscono dispositivi a sé stanti (continua)

REQUISITI RELATIVI ALLA PROGETTAZIONE E ALLA FABBRICAZIONE

- 17.1 I dispositivi contenenti sistemi elettronici programmabili, compresi i software, o i software che costituiscono dispositivi a sé stanti, sono progettati in modo tale da garantire la riproducibilità, l'affidabilità e le prestazioni in linea con la destinazione d'uso per essi prevista. In caso di condizione di primo guasto sono previsti mezzi adeguati per eliminare o ridurre, per quanto possibile, i rischi che ne derivano o il peggioramento delle prestazioni.
- 17.2 Per i dispositivi contenenti un software o per i software che costituiscono dispositivi a sé stanti, il software è sviluppato e fabbricato conformemente allo stato dell'arte, tenendo conto dei principi del ciclo di vita dello sviluppo, della gestione del rischio, compresa la sicurezza delle informazioni, della verifica e della convalida.

REQUISITI RELATIVI ALLA PROGETTAZIONE E ALLA FABBRICAZIONE

- 17.3 I software di cui al presente punto destinati a essere usati in combinazione con piattaforme di calcolo mobili sono progettati e fabbricati tenendo conto delle peculiarità della piattaforma mobile (ad esempio dimensioni e grado di contrasto dello schermo) e di fattori esterni connessi al loro uso (variazioni ambientali relative al livello di luce o di rumore). Mobile health ??? App ??
- 17.4. I fabbricanti indicano requisiti minimi in materia di hardware, caratteristiche delle reti informatiche e misure di sicurezza informatica, compresa la protezione contro l'accesso non autorizzato, necessari per far funzionare il software come previsto. 80001 ??

Capo III – Regole di Classificazione

6 Dispositivi attivi

6.3 Regola 11

Il software destinato a fornire informazioni utilizzate per prendere decisioni a fini diagnostici o terapeutici rientra nella classe IIa, a meno che tali decisioni abbiano effetti tali da poter causare:

- il decesso o un deterioramento irreversibile delle condizioni di salute di una persona, nel qual caso rientra nella classe III, o
- un grave deterioramento delle condizioni di salute di una persona o un intervento chirurgico, nel qual caso rientra nella classe IIb.
- Il software destinato a monitorare i processi fisiologici rientra nella classe IIa, a meno che sia destinato a monitorare i parametri fisiologici vitali, ove la natura delle variazioni di detti parametri sia tale da poter creare un pericolo immediato per il paziente, nel qual caso rientra nella classe IIb.
- Tutti gli altri software rientrano nella classe I.

SENTENZA DELLA CORTE DI GIUSTIZIA UE (Quarta Sezione) - 7 dicembre 2017

L'associazione francese Sniterm (imprese tecnologia medicale), ha chiesto al giudice di primo grado e poi alla Corte di Giustizia di valutare se il software che presenti "una funzionalità che consenta l'utilizzo dei dati personali di un paziente al fine di aiutare il suo medico nella predisposizione della sua prescrizione, in particolare rilevando le controindicazioni, le interazioni con altri medicinali e le posologie eccessive" debba o meno essere considerato dispositivo medico, tenuto conto in particolare che lo stesso non risulta impiegato "nel" o "sul" corpo umano. In sostanza si chiedeva alla Corte di stabilire se, per la qualificazione di un software come dispositivo medico, occorre che il software stesso debba essere destinato dal fabbricante ad essere necessariamente "impiegato sull'uomo.

I principi espressi dalla Corte di giustizia, ai fini della qualifica di un software come dispositivo medico:

- non è sufficiente che lo stesso sia utilizzato in un contesto medico, ma occorre invece che il fabbricante abbia destinato il software ad una diretta e specifica finalità medica;
- il legislatore dell'Unione ha inteso concentrarsi, per qualificare un software come dispositivo medico, sullo scopo del suo utilizzo e non sul modo in cui può concretizzarsi l'effetto che è in grado di produrre sul o nel corpo umano": ne consegue che "ai fini della qualificazione di dispositivo medico, il fatto che un software agisca direttamente o non agiscano direttamente sul corpo umano, non è rilevante, essendo invece fondamentale che la finalità indicata dal fabbricante sia una di quelle previste per la definizione stessa di dispositivo".

Destinazione d’uso

Questi grafici sono visualizzazioni progettate per mostrare le tendenze generali dei dati ricevuti dal dispositivo di origine e non devono essere utilizzati per diagnosticare o trattare condizioni mediche.

Regolamento Privacy

Registro delle attività di trattamento

- Obbligo di tenuta di un **registro delle attività di trattamento** sia per il **titolare** che per il **responsabile**, in caso di imprese o organizzazioni con 250 o più dipendenti
- Il registro deve essere tenuto **in forma scritta**, anche in formato elettronico

Responsabili trattamento, data protection officer

- La nomina del responsabile deve essere formalizzata mediante un **apposito contratto o altro atto giuridico** che disciplini i trattamenti di dati effettuati dal responsabile per conto del titolare (cfr. art. 28 Reg. EU 2016/679).
- Obbligo di nomina del **Responsabile della Protezione dei dati o Data Protection Officer (DPO)**

Data breach

- Obbligo di **notifica della violazione dei dati personali** (Data Breach) entro termini temporali stringenti

Alcuni dati economici

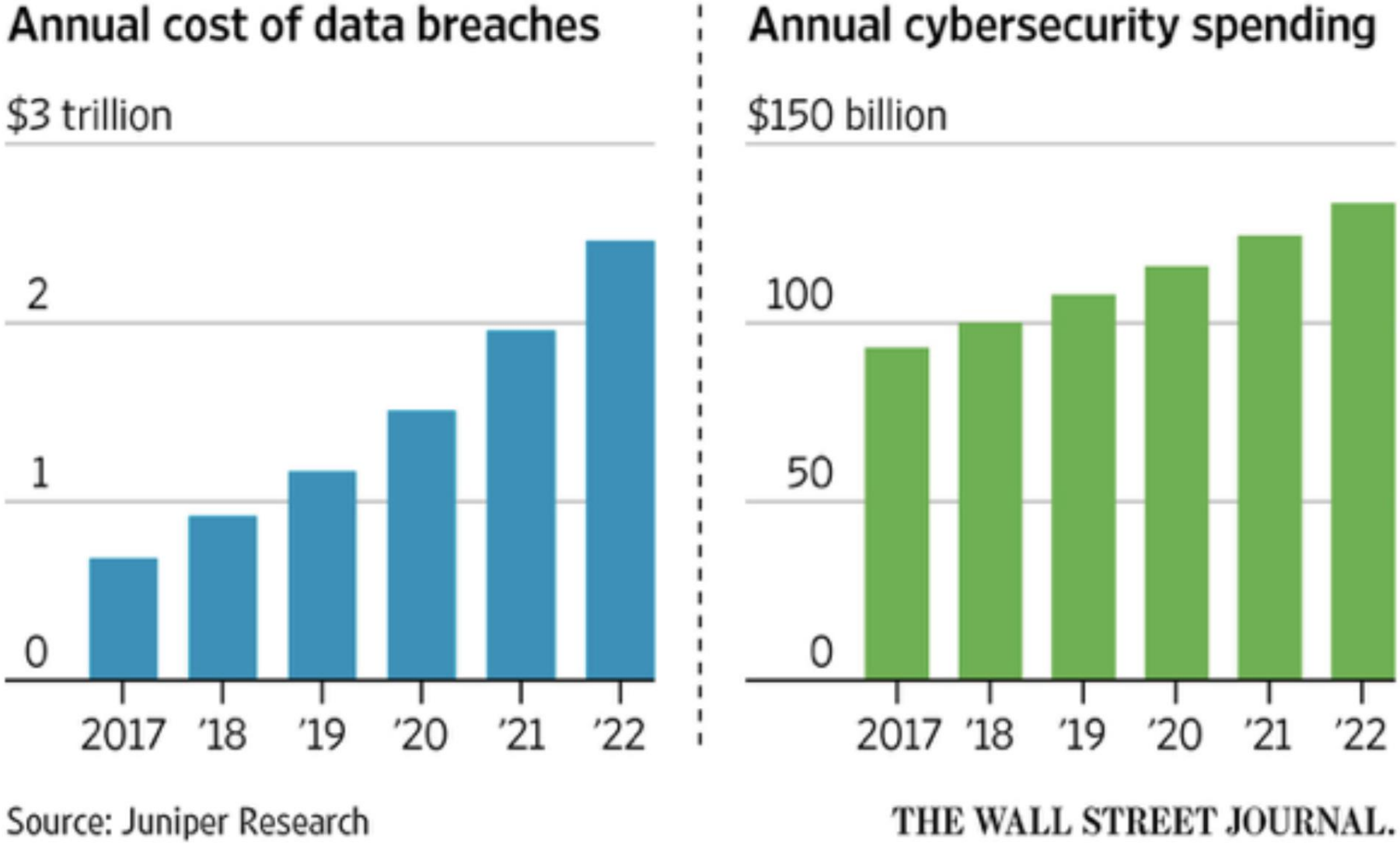
- Spesa in cybersecurity globale 100 B$
- Perdite globali di business dovute ad incidenti cyber 1000 B$
- Nel 2008 si stima siano stati introdotti 1 M di nuovi virus (dati Symantec)
- Nel 2016 1M al giorno (Symantec's 2017 Internet Security Threat Report ISTR)
- il valore di una carta di credito rubata (da 0,5 $ fino a 60$)
- Valore di un medical record rubato (da 1 $ fino a 22$)
- Un cyber attacco globale può causare perdite per 53 B$ comparabile con una catastrofe naturale (es. tempesta Sandy 2012) (es. Wannacry 8 B$)

Rif: (Symantec's 2017 Internet Security Threat Report ISTR)

FAIR Institute Blog. Cyber Economics: Smarter (vs. More Expensive) Cybersecurity

Growing Threat

Estimated increases in data-breach costs and global cybersecurity spending over the next five years



Source: Juniper Research

THE WALL STREET JOURNAL.

Conclusioni

- Attenzione al problema Cybersecurity in crescita
- I dispositivi medici sono sempre più interconnessi e dislocati e presentano peculiarità che richiedono un particolare trattamento
- Aumenta pericolo di:
  - Malfunzionamento dispositivi
  - Interruzione di servizi sanitari
  - Mancato accesso ad informazioni sul paziente
  - Mancato accesso o compromissione della cartella elettronica
- la difesa dagli attacchi di malware richiede un approccio proattivo che coinvolge l'alta direzione, l'ingegneria clinica, l'IT e le persone in tutta l'organizzazione sanitaria