# L'ingegnere clinico e i dispositivi medici in una rete IT-Medicale

Ing. Maurizio Rizzetto

REGIONE AUTONOMA FRIULI VENEZIA GIULIA
ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO
Burlo Garofolo di Trieste
BURLO

# 21st Century Health Sustainability of Medical Systems *Common international themes*

- da servizi basati sul volume a servizi basati sulla gestione della salute della popolazione
- tema dell'età e multimorbidità
- Successo nell'aumento della vita media non sempre con adeguata qualità della stessa
- Crescente complessità dei percorsi di cura e difficoltà nel fornire cure di qualità costante
- Mancanza di interoperabilità dei sistemi clinici e difficoltà nella condivisione dei dati
- Forza lavoro e burnout

Charles Alessi
Chief Clinical Officer HIMSS

# Solutions
# Interoperability and Precision Medicine

- Evidence based care customised to the individual. “For me”
- Encouraging active engagement and participation of patients own care
- Encourage use of digital technologies as “clinical extenders”
- Develop and use registries that assist Clinicians to reduce unwarranted variation
- Predictive approaches – Genomics and Biologics
- Insights – IOT
- Deployment of AI solutions at scale and pace

Charles Alessi
Chief Clinical Officer HIMSS

# Global and local impact Systems and Device

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



Rif. Yadin David BAC

# Apparecchio per Anestesia ANS

Siemens Servo 900 c (anno 1981)

IERI

Dräger Perseus® A500

OGGI


FDA-cleared and CE mark

# Sfide organizzative

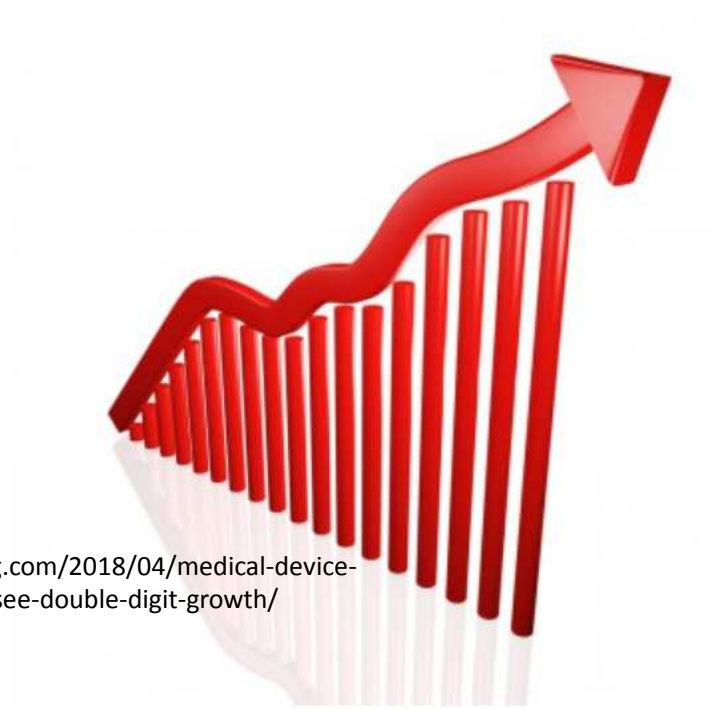
- La Crescita esponenziale della complessità delle tecnologie e loro necessità di connettività hanno prodotto “sistemi di sistemi” che richiedono organizzazioni a supporto molto diverse di quelle richieste per le precedenti generazioni di apparecchiature sanitarie.
- Le tecnologie sanitarie e quelle dell’informazione sono state fino a poco tempo fa supportate da diversi gruppi provenienti da diversi percorsi formativi e culturali…. Questi gruppi devono trovare un nuovo assetto al fine di garantire una corretta gestione delle nuove tecnologie nei nuovi contesti sanitari
- Le conoscenze, le abilità e le capacità necessarie per supportare i professionisti sanitari nel gestire le nuove tecnologie sanitarie non sono al passo con l'evoluzione esponenziale della tecnologia.
- I servizi a supporto nella gestione delle tecnologie sanitarie hanno spesso risorse limitate, in un numero insufficiente e con una combinazione inadeguata di responsabili, ingegneri e tecnici.



INDUSTRY NEWS

# Medical Device Connectivity Market to See Double-Digit Growth

Published on April 27, 2018



http://www.24x7mag.com/2018/04/medical-device-connectivity-market-see-double-digit-growth/

# The List for 2019

1. *Hackers Can Exploit Remote Access to Systems, Disrupting Healthcare Operations*
2. *"Clean" Mattresses Can Ooze Body Fluids onto Patients*
3. *Retained Sponges Persist as a Surgical Complication Despite Manual Counts*
4. *Improperly Set Ventilator Alarms Put Patients at Risk for Hypoxic Brain Injury or Death*
5. *Mishandling Flexible Endoscopes after Disinfection Can Lead to Patient Infections*
6. *Confusing Dose Rate with Flow Rate Can Lead to Infusion Pump Medication Errors*
7. *Improper Customization of Physiologic Monitor Alarm Settings May Result in Missed Alarms*
8. *Injury Risk from Overhead Patient Lift Systems*
9. *Cleaning Fluid Seeping into Electrical Components Can Lead to Equipment Damage and Fires*
10. *Flawed Battery Charging Systems and Practices Can Affect Device Operation*

ECRI Institute

2019 Top 10
Health Technology Hazards

A Report from Health Devices

www.ecri.org/2019hazards

ECRI Institute

SPECIAL REPORT

# Top 10 Health Technology Hazards for 2020

## Expert Insights from Health Devices

## Executive Brief

ECRI Institute is providing this abridged version of its 2020 Top 10 list of health technology hazards as a free public service to inform healthcare facilities about important safety issues involving the use of medical devices and systems. The full report—including detailed problem descriptions and ECRI Institute's step-by-step recommendations for addressing the hazards—is available to members of ECRI Institute programs through their membership web pages.

### The List for 2020

1. Misuse of Surgical Staplers
2. Adoption of Point-of-Care Ultrasound Is Outpacing Safeguards
3. Infection Risks from Sterile Processing Errors in Medical and Dental Offices
4. Hemodialysis Risks with Central Venous Catheters—Will the Home Dialysis Push Increase the Dangers?
5. Unproven Surgical Robotic Procedures May Put Patients at Risk
6. Alarm, Alert, and Notification Overload
7. Cybersecurity Risks in the Connected Home Healthcare Environment
8. Missing Implant Data Can Delay or Add Danger to MRI Scans
9. Medication Errors from Dose Timing Discrepancies in EHRs
10. Loose Nuts and Bolts Can Lead to Catastrophic Device Failures and Severe Injury



SEVEN

7

## Cybersecurity Risks in the Connected Home Healthcare Environment

Remote patient monitoring technologies are increasingly being used for at-home monitoring to help clinicians identify deteriorating patients before they require hospitalization. As network-connected medical technologies such as these move into the home, cybersecurity policies and practices that address the unique challenges involved must be instituted as well.

As with any networked medical device, connected devices used in the home must be protected against threats that could interrupt the flow of data, alter or degrade the device's performance, or expose protected health information. A cybersecurity issue that interrupts the transfer of data to the healthcare provider, for example, could lead to misdiagnosis or a delay in care.

Challenges include: the deployment may rely on the patient's home network, which the provider doesn't control; physical access to the device is limited, which can complicate trouble-shooting and installing updates; and patient compliance can be difficult to sustain, particularly if the patient lacks proficiency using the device or has unwarranted fears about cyberse-curity risks.

Recommendations include assessing system security during device procurement and addressing security considerations during installation, both at the patient's home and on the provider's network. The goal is not just to get the monitoring system to function, but to get it functioning securely.

> Connected devices used in the home must be protected against threats that could interrupt the flow of data, alter or degrade the device's performance, or expose protected health information.

# Solutions and Challenges
# The Hospital environments

- From departmental models to interdependencies. ( Model of Odense Denmark)
- Increasing numbers of touch points for patients requiring a “single version of the truth” —- Inter-operability and inter-dependence
- Ingestion of non biomedical data to drive personalised prevention
- Data and clinical governance – doing things the same way
- Clinical Engineers no longer “in the cupboard under the stairs”
- Laboratories at the vanguard of change – they have the insights
- Reaching out to the community – the hospitals without walls

REGIONE AUTONOMA FRIULI VENEZIA GIULIA
ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO
Burlo Garofolo di Trieste
BURLO

Charles Alessi
Chief Clinical Officer HIMSS

# ADVANCING CYBERSECURITY OF HEALTH AND DIGITAL TECHNOLOGIES MARCH 2019

## COCIR SUSTAINABLE COMPETENCE IN ADVANCING HEALTHCARE

European Coordination Committee of the Radiological, Electromedical and Healthcare IT Industry

- Documento sviluppato da COCIR per garantire che VENDORS e USERS possano applicare correttamente i regolamenti e le norme tecniche vigenti nei paesi membri
- La sicurezza è una responsabilità condivisa
- Un prodotto/servizio deve rispondere a specifici requisiti di sicurezza e consentire il controllo della rispondenza nel tempo ai requisiti stessi secondo quanto previsto dalle normative


*Figure 1: Overview of the framework for cybersecurity in Europe's health sector*

SECURITY BY DESIGN

A seguito di aumento del rischio cyber per apparecchiature interconnesse sia nelle strutture sanitarie che nelle applicazioni domiciliari

# Le norme

- MDR regolamento dispositivi medici
- NIS Direttiva del 2016 ma recepita dagli stati membri nel 2018
  - Ogni stato membro ha individuato un CSIRT (computer security Incident Response Team) (CERT Computer Emergency Response Team)
  - La commissione europea e l'agenzia per la cybersicurezza ENISA coordinano
- GDPR in vigore da maggio 2018
- Cybersecurity ACT
  - Certificazione dei prodotti/servizi sicuri (ogni stato membro nomina un autorità)
- Standard internazionali



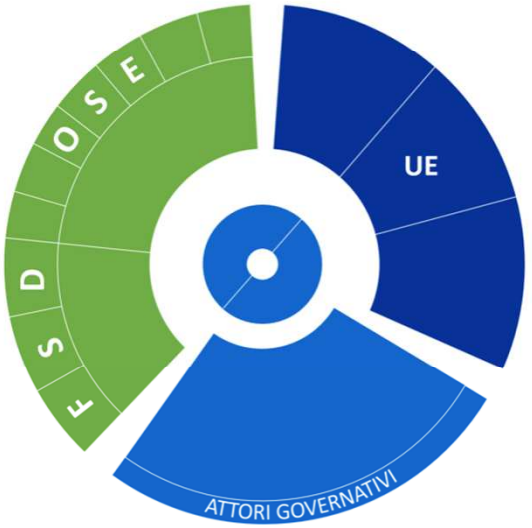
Computer Security Incident Response Team Italia

HOME DIRETTIVA NIS MODULISTICA NORMATIVA CONTATTI

COMPUTER EMERGENCY RESPONSE TEAM PUBBLICA AMMINISTRAZIONE
CERT - PA

CERT nazionale Italia

# CSIRT Italia




CHI SIAMO

COSA FACCIAMO

NOTIFICA INCIDENTE

CERT nazionale Italia

COMPUTER EMERGENCY RESPONSE TEAM

MINISTERO DELLO SVILUPPO ECONOMICO

Link Utili FAQ Glossario

Home Chi siamo News Bollettini Documenti Contatti

Ricerca:

# CERT Nazionale Italia

La crescente esigenza di garantire capacità di prevenzione e reazione ad eventi cibernetici richiede lo sviluppo di CERT (Computer Emergency Response Team) quali soggetti erogatori di servizi di supporto, formazione, informazione, ricerca e sviluppo per i rispettivi utenti, pubblici o privati. Il CERT Nazionale supporta la costituzione di una community per la sicurezza nazionale.

## News

VULNERABILITÀ

### Vulnerabilità di tipo DoS in ISC Bind 9

BIND denial-of-service 22 novembre 2019

È stata riscontrata una vulnerabilità di media gravità in ISC BIND 9 che può causare condizioni di denial of service. Leggi tutto

## Bollettini

### Bollettino IT-CERT.190527.B01 Vulnerabilità critica in IBM WebSphere Application Server

| | |
|---|---|
| Gravità (CVSS) | 9,0 |
| Prima emissione | 27 maggio 2019 |
| Ultima modifica | - |

REGIONE AUTONOMA FR
ISTITUTO DI RICOVERO E
A CARATTERE SCIENTIFIC
Burlo Garofolo di T

enisa
Homepage
EUROPEAN UNION AGENCY FOR CYBERSECURITY

TOPICS | NEWS | PUBLICATIONS | EVENTS 3 | English (en)

About ENISA Careers 4 Procurement 1 Contact

## ENISA Topics

- Cloud and Big Data
- Critical Infrastructures and Services
- CSIRT Services
- CSIRTs and communities
- CSIRTs in Europe
- Cyber Crisis Management
- Cyber Exercises
- Cybersecurity Education
- Data Protection
- Incident Reporting
- IoT and Smart Infrastructures
- National Cybersecurity Strategies
- NIS Directive
- Standards and Certification
- Threat and Risk Management
- Trainings for Cybersecurity Specialists
- Trust Services

## Latest news All news


PRESS RELEASE
### ENISA draws Threat Landscape of 5G Networks

ENISA, the European Union Agency for Cybersecurity publishes a Threat Landscape for 5G Networks, assessing the threats related to the fifth generation of mobile telecommunications networks (5G).

Published on November 21, 2019. Read more

**New Executive Board Member**
Published on November 21, 2019

PRESS RELEASE
**ENISA draws Threat Landscape of 5G Networks**
Published on November 21, 2019

PRESS RELEASE
**How to implement security by design for IoT**
Published on November 19, 2019

**29th Article 13a telecom security meeting in Belgrade**
Published on November 18, 2019

**GDPR & deploying pseudonymisation techniques**
Published on November 15, 2019

CERT nazionale Italia
COMPUTER EMERGENCY RESPONSE TEAM

MINISTERO DELLO SVILUPPO ECONOMICO

Link Utili FAQ Glossario

Home Chi siamo News Bollettini Documenti Contatti

Ricerca:

Home » News » Vulnerabilità in Philips IntelliVue MX40 Patient Worn Monitor (WLAN)

VULNERABILITÀ

# VULNERABILITÀ IN PHILIPS INTELLIVUE MX40 PATIENT WORN MONITOR (WLAN)

Philips venerdì, 15 settembre 2017

ICS-CERT, il CERT americano dedicato ai sistemi di controllo industriali, ha recentemente pubblicato l'*advisory* ICSMA-17-255-01 (in Inglese) riferito a vulnerabilità software relative al prodotto **Philips IntelliVue MX40 Patient Worn Monitor**, un monitor paziente indossabile che utilizza la rete locale *wireless* per scambiare i dati con la stazione centrale di monitoraggio, raccomandandone la diffusione presso gli utilizzatori vista la natura del dispositivo.


Philips IntelliVue MX40

Le vulnerabilità in questione (CVE-2017-9657 e CVE-2017-9658), sotto specifiche condizioni, potrebbero rendere possibile forzare un funzionamento anomalo del dispositivo.

# Security Advisory & Archive

Philips CT Imaging System Vulnerabilities (1-MAY-2018)

Publication Date: May 1, 2018
Update Date: May 1, 2018

Philips is a committed leader in medical device cybersecurity. As part of our global Product Security Policy, the company conducts extensive ongoing analysis of our products, often in collaboration with customers and researchers, to identify and address potential vulnerabilities.

As part of Philips' Responsible Disclosure Policy for the awareness and remediation of identified product security vulnerabilities, the company is proactively issuing an advisory concerning a potential, low-risk security vulnerability that may affect the following Philips Computed Tomography (CT) imaging systems:

- Brilliance 64 version 2.6.2 and below
- Brilliance iCT versions 4.1.6 and below
- Brillance iCT SP versions 3.2.4 and below
- Brilliance CT Big Bore 2.3.5 and below

Philips has confirmed that the potential security vulnerability, if successfully exploited, may allow an attacker to gain unauthorized access to elevated privileges and/or restricted system resources and information. This vulnerability is not exploitable remotely and cannot be exploited without user interaction, and an attacker would need local access to the kiosk environment of the medical device to be able to implement the exploit.

At this time, Philips has received no reports of exploitation of this vulnerability or incidents from clinical use that have been associated with the vulnerability.



| | | | | | | |
|---|---|---|---|---|---|---|
| Italy | CERTBI | Financial | Not member | Accredited | Not member | cert.bancadital… |
| Italy | CERT-PA | Government | Not member | Accredited | Not member | cert-pa.it/ |
| Italy | CERT-ENAV | CIIP | Not member | Accredited | Member | enav.it/sites/p… |
| Italy | CERT-Difesa | Military | Not member | Not listed | Not member | difesa.it/SMD_… |
| Italy | CERT-RAFVG | Local Agencies | Not member | Not listed | Not member | cert-rafvg.regi… |
| Italy | YOROI-CSDC | Commercial Organisation | Not member | Accredited | Not member | yoroi.company/ |
| Italy | D3Lab CERT Team | Commercial Organisation | Not member | Listed | Not member | d3lab.net/ |
| Italy | GARR-CERT | NREN | Not member | Accredited | Not member | cert.garr.it |
| Italy | PI-CERT | Commercial Organisation, Financial, Government | Not member | Accredited | Member | picert.it |
| Italy | IT-CERT | Government, National | Member | Accredited | Not member | certnazionale.it/ |
| Italy | CERTEGO-IRT | Commercial Organisation | Not member | Listed | Member | Public website not available |
| Italy | LDO-CERT | CIIP | Not member | Accredited | Not member | leonardocomp… |
| Italy | Enel CERT | Energy | Not member | Accredited | Member | enel.com/ |
| Italy | SIA CERT | Financial | Not member | Listed | Not member | sia.eu/en/cert |
| Italy | TS-WAY CIOC | Service Provider Customer Base | Not member | Listed | Not member | Public website not available |
| Italy | TERNA-CERT | CIIP | Not member | Accredited | Not member | terna.it/en-gb/… |
| Italy | SOC-GSE | Government | Not member | Listed | Not member | Public website not available |
| Italy | YCERT | Commercial Organisation, Service Provider Customer Base | Not | Listed | Member | yarix.com |

SIEMENS

Search for...

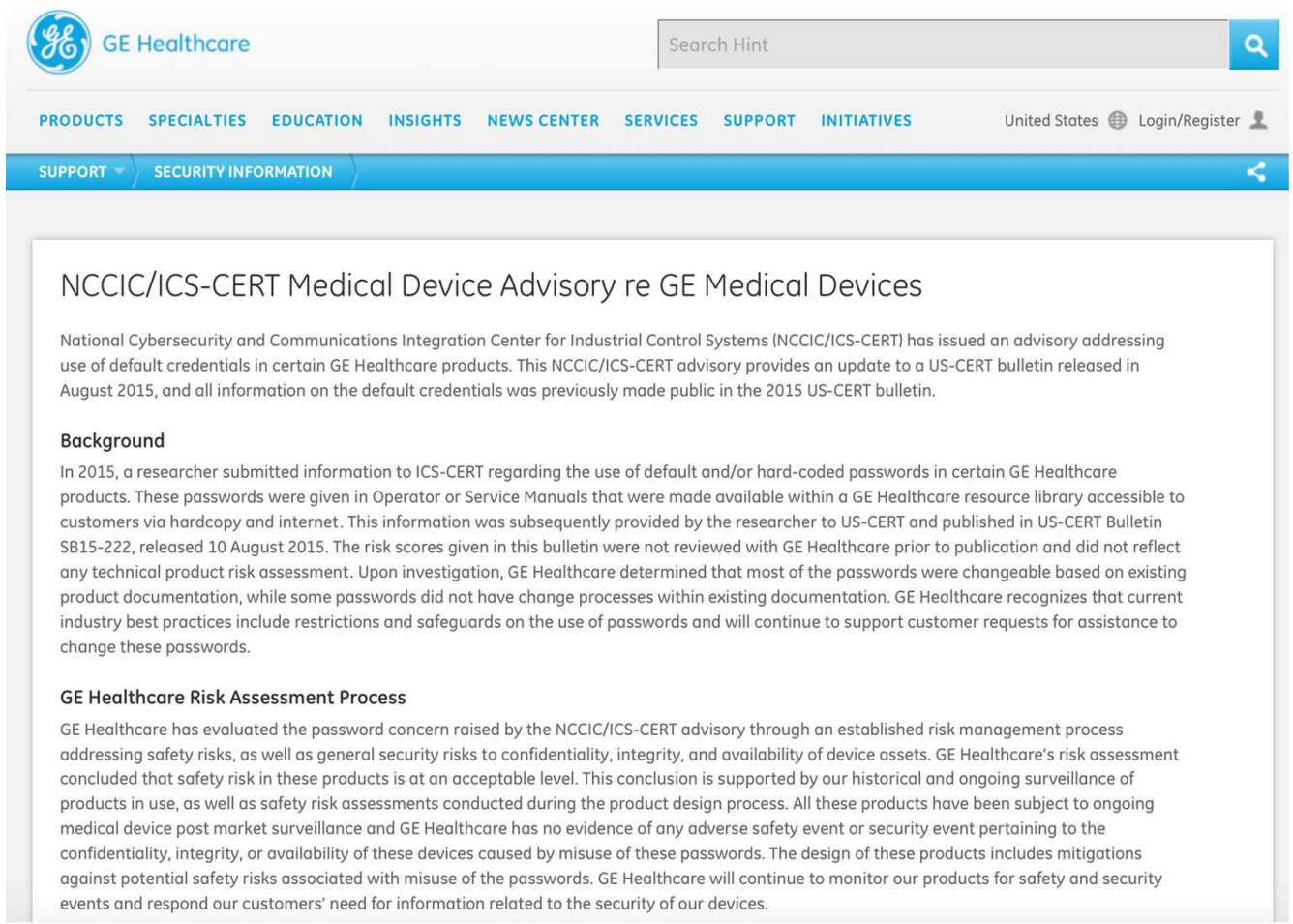
# Siemens ProductCERT and Siemens CERT


**The central expert teams for immediate response to security threats and issues affecting Siemens products, solutions, services, or infrastructure.**

**Siemens ProductCERT** is a dedicated team of seasoned security experts that manages the receipt, investigation, internal coordination, and public reporting of security issues related to Siemens products, solutions, or services. ProductCERT cultivates strong and credible relationships with partners and security researchers around the globe to advance Siemens product security, to enable and support development of industry best practices, and most importantly to help Siemens customers manage security risks.
The team acts as the central contact point for security researchers, industry groups, government organizations, and vendors to report potential Siemens product security vulnerabilities. This team will coordinate and maintain communication with all involved parties, internal and external, in order to appropriately respond to identified security issues. Security Advisories are released in order to inform customers about necessary steps to securely operate Siemens products and solutions.

**Siemens CERT** is a dedicated team of Security Engineers with the mission to secure the Siemens infrastructure. CERT monitors the current Cyber Threat Landscape for Siemens and assesses its potential impact to the enterprise. Based on that know-how and the latest technological trends, it consults the Information Technology department in Siemens to improve the enterprise IT Security. The team is responsible for coordinating the response to Cyber Security Incidents within Siemens.
To achieve its mission, CERT leverages the relationships with various internal and external stakeholders world-wide, such as CSIRT networks, technical communities, and the security researcher communities. CERT is also recognized as a trusted research partner by academia and industry, with numerous projects and publications in its expert area.

Know the Issues. Know the Mitigations.



GE Healthcare

Search Hint

PRODUCTS SPECIALTIES EDUCATION INSIGHTS NEWS CENTER SERVICES SUPPORT INITIATIVES United States Login/Register

SUPPORT SECURITY INFORMATION

## NCCIC/ICS-CERT Medical Device Advisory re GE Medical Devices

National Cybersecurity and Communications Integration Center for Industrial Control Systems (NCCIC/ICS-CERT) has issued an advisory addressing use of default credentials in certain GE Healthcare products. This NCCIC/ICS-CERT advisory provides an update to a US-CERT bulletin released in August 2015, and all information on the default credentials was previously made public in the 2015 US-CERT bulletin.

### Background

In 2015, a researcher submitted information to ICS-CERT regarding the use of default and/or hard-coded passwords in certain GE Healthcare products. These passwords were given in Operator or Service Manuals that were made available within a GE Healthcare resource library accessible to customers via hardcopy and internet. This information was subsequently provided by the researcher to US-CERT and published in US-CERT Bulletin SB15-222, released 10 August 2015. The risk scores given in this bulletin were not reviewed with GE Healthcare prior to publication and did not reflect any technical product risk assessment. Upon investigation, GE Healthcare determined that most of the passwords were changeable based on existing product documentation, while some passwords did not have change processes within existing documentation. GE Healthcare recognizes that current industry best practices include restrictions and safeguards on the use of passwords and will continue to support customer requests for assistance to change these passwords.

### GE Healthcare Risk Assessment Process

GE Healthcare has evaluated the password concern raised by the NCCIC/ICS-CERT advisory through an established risk management process addressing safety risks, as well as general security risks to confidentiality, integrity, and availability of device assets. GE Healthcare's risk assessment concluded that safety risk in these products is at an acceptable level. This conclusion is supported by our historical and ongoing surveillance of products in use, as well as safety risk assessments conducted during the product design process. All these products have been subject to ongoing medical device post market surveillance and GE Healthcare has no evidence of any adverse safety event or security event pertaining to the confidentiality, integrity, or availability of these devices caused by misuse of these passwords. The design of these products includes mitigations against potential safety risks associated with misuse of the passwords. GE Healthcare will continue to monitor our products for safety and security events and respond our customers' need for information related to the security of our devices.

| PRE-MARKET PROCESS | PRODUCT FEATURES | DOCUMENTS | POST-MARKET PROCESS |
|---|---|---|---|
| ESTABLISH SECURE DEVELOPMENT LIFECYCLE | BUILD PRODUCTS WITH THE APPROPRIATE SECURITY CONTROLS | SPECIFY SECURE USE | SECURITY MANAGEMENT (UPDATES AND UPGRADES |

**ISO 27034 IEC 62443-4-1 *IEC 62304*, 82304, 80001-5-1****

**NIST FIPS 199 Security Categorization**

**Threat / Risk Analysis**
***ISO 14971****
**NIST SP800-30**
**IEC 62443-3-2***
**ISO 20004**
**ISO 27005**
**ISO 31000**

***IEC 60601-1 SafetyEN 45502-1 & ISO 14708-1***
***Active implants***
***ISO 22696 PHD Identification & Authentication***
***IEC 60601-4-5 Safety related security spec****
***ISO 11633-1/2 Remote ServiceISO 13606-4 EHR***
***IHE IT Infrastructure Profiles***
**NIST SP800-53 Security Controls**
**ISO 15408 Common Criteria**

**ISO 15026-1/2**
**Assurance case**

**ISO 15443-1/2**
**Security assurance**

***IEC 80001-2-2***
***IEC 80001-2-8***
***IEC 80001-2-9***
***HIMSS NEMA MDS2****
***CLSI AUTO-11-A2***

**ISO/IEC 29417 Disclosure**
**ISO/IEC 30111 Vul./Incident**

**ISO 270xx Information Security Management**
(Product operations)

**ISO 270xx (Lifecycle)**
**ISO 12207**
**ISO 15228**
**NIST SP800-160**
**SAFECode**
**OWASP**
**MITRE CWE & CAPEC**

**ISO**
**18004 Timestamps**
**18033 Encryption**
**18367 Crypto algorithms**
**18370 Digital Signatures**
**19592 Secret Sharing**
**19772 Auth. encryption**
**27040 Secure Storage**

**NIST FIPS**
**140-2 Crypto Mod**
**180-4 Hashing**
**186-4 Digital Signatures**
**193 Platform Resilience**
**197 Encryption**
**198-1 Hash Msg Auth**
**200 Min Security Reqmts**
**201 Person Authentic**
**202 SHA-3**

***Black italic*** = Healthcare specific
***** = New or being revised

## ANNEX 1.
## SECURITY REQUIREMENTS IN MEDICAL DEVICE REGULATION

| **ORGANIZATION:**<br>**STATE OF THE ART INFORMATION SECURITY MANUFACTURING**<br>ANNEX I.17.2 | | | | | |
|---|---|---|---|---|---|
| Device:<br>**ENVIRONMENT**<br>Annex I.14.2(d) | Device:<br>**REPEATABILITY**<br>Annex I.17.1 | Device:<br>**RELIABILITY**<br>Annex I.17.1 | Device:<br>**PERFORMANCE**<br>Annex I.17.1 | Device:<br>**ACCESS CONTROL**<br>Annex I.17.4<br>Annex I.18.8 | Labeling:<br>**SECURITY MEASURES & NETWORK CHARACTERISTICS**<br>Annex I.17.4<br>Annex I.23.4(ab) |

# Regolamento europeo Cybersecurity Act

7.6.2019 IT Gazzetta ufficiale dell'Unione europea L 151/15

**REGOLAMENTO (UE) 2019/881 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO**

**del 17 aprile 2019**

**relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cibersicurezza»)**

**(Testo rilevante ai fini del SEE)**

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea, in particolare l'articolo 114,

vista la proposta della Commissione europea,

previa trasmissione del progetto di atto legislativo ai parlamenti nazionali,

visto il parere del Comitato economico e sociale europeo ([1]),

visto il parere del Comitato delle regioni ([2]),

deliberando secondo la procedura legislativa ordinaria ([3]),

considerando quanto segue:

(1) Le reti e i sistemi informativi e le reti e i servizi di comunicazione elettronica svolgono un ruolo essenziale nella società e sono diventati i pilastri della crescita economica. Le tecnologie dell'informazione e della comunicazione (TIC) sono alla base dei sistemi complessi su cui poggiano le attività quotidiane della società, fanno funzionare le nostre economie in settori essenziali quali la sanità, l'energia, la finanza e i trasporti e, in particolare, contribuiscono al funzionamento del mercato interno.

(2) L'uso delle reti e dei sistemi informativi da parte di cittadini, organizzazioni e imprese di tutta l'Unione è attualmente molto diffuso. La digitalizzazione e la connettività stanno diventando caratteristiche fondamentali di un numero di prodotti e servizi in costante aumento, e con l'avvento dell'Internet degli oggetti (*Internet of Things* — IoT) nel prossimo decennio dovrebbero essere disponibile in tutta l'Unione un numero estremamente elevato di dispositivi digitali connessi. Sebbene un numero crescente di dispositivi sia connesso a Internet, la sicurezza e la resilienza non sono sufficientemente integrate nella progettazione, il che rende inadeguata la cibersicurezza. In tale contesto, l'uso limitato della certificazione fa sì che gli utenti individuali, nelle organizzazioni e nelle aziende dispongano di informazioni insufficienti sulle caratteristiche dei prodotti TIC, dei servizi TIC e dei processi TIC in termini di cibersicurezza, il che mina la fiducia nelle soluzioni digitali. La rete e i sistemi informativi sono in grado di aiutarci in tutti gli aspetti della vita e danno impulso alla crescita economica dell'Unione. Sono fondamentali per il raggiungimento del mercato unico digitale.

**Il Regolamento è stato pubblicato in Gazzetta Ufficiale il 7 giugno 2019 ed è entrato in vigore il 27 giugno 2019**

# L'approccio dell'ingegnere clinico ……

É in pericolo la salute del paziente ?

La salute del paziente e
la sua sicurezza hanno la priorità !

# I dispositivi medici in un tipico ospedale

- Un ospedale di 500 pl ha circa 7000 apparecchiature medicali (con presenza di alcune migliaia di modelli e centinaia se non migliaia di diversi fornitori/fabbricanti)

- Classificazione in due categorie: apparecchiature diagnostiche e terapeutiche

# Conseguenze di una compromissione Cyber

- Errata diagnosi e conseguente errato trattamento sanitario
- Ritardo nella diagnosi e conseguente ritardo nel trattamento
- Possibile perdita diffusione di dati personali/sensibili del paziente
- Danno all'apparecchiatura medica e conseguente sua indisponibilità



# Criticità cyber per i DM

- Caso di compromissione di molte apparecchiature dello stesso tipo (pompe infusionali, ecc.)

- Caso di gruppi più piccoli o singole apparecchiature che però possono avere elevato impatto sulla salute e sulla vita del paziente. (DM life support)

# Dispositivi connessi in rete ed interoperabili

- Ogni dispositivo medico connesso in rete e interoperabile con altri sistemi può essere causa di vulnerabilità cyber sull'intero sistema. Puo' in altri termini costituire un *single point of failure* (SPoF),
- L'introduzione di innovazioni quali machine learning (ML) and artificial intelligence (AI) richiedono una forte integrazione dei dati e portano ad una modifica dei processi di cura e a nuovi rischi in caso di indisponibilità degli stessi.

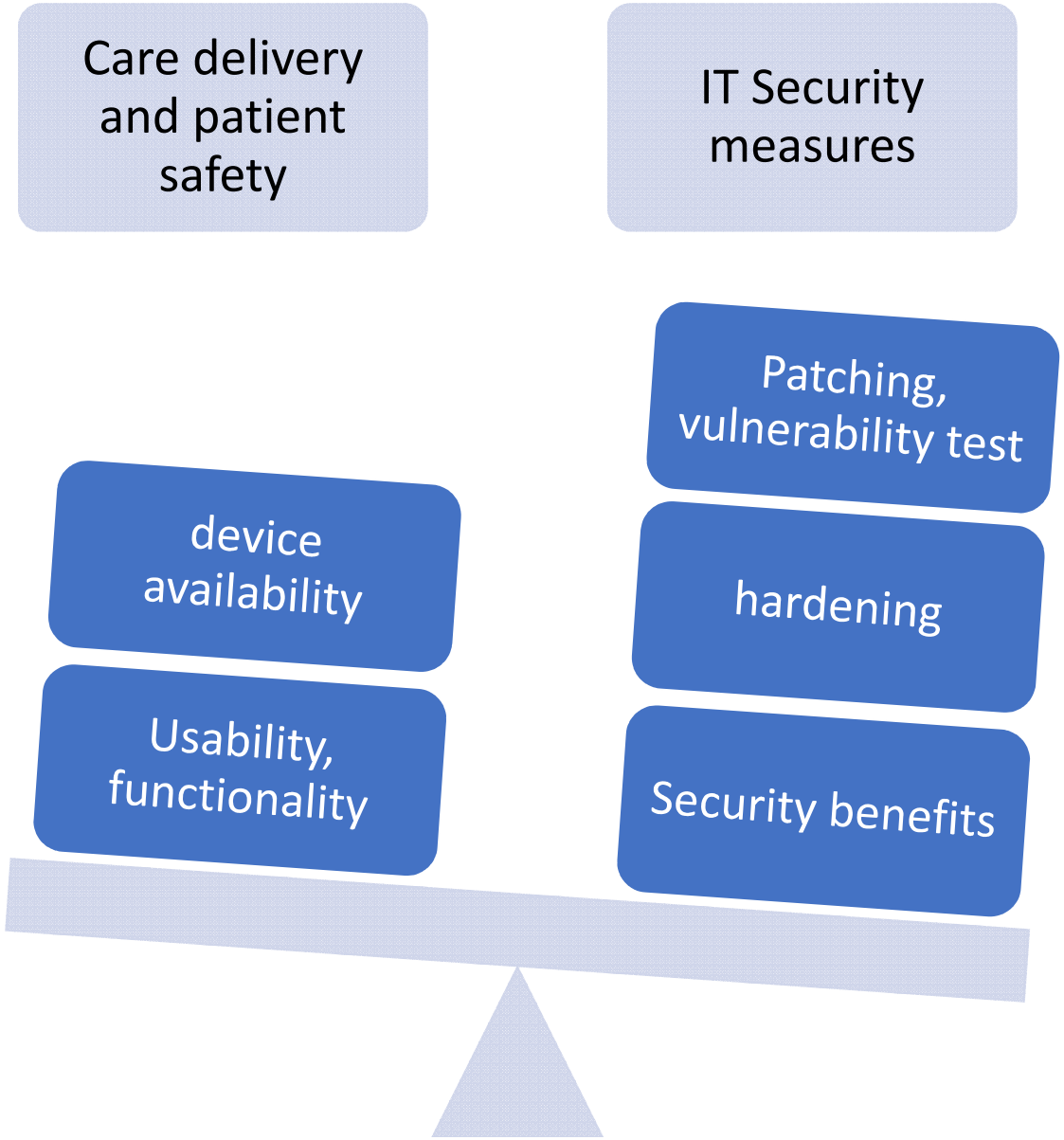


# Dimensioni esposizione MD

- 10-15 M Dispositivi Medici MD in USA
- 25-40% of MD sono collegate in rete
- 2,5-6 M of MD a rischio di attacchi Cyber

# MD da a apparecchi fissi a dispositivi mobili interoperabili

In passato i dispositivi medici si trovavano fissi in ambulatorio o specifici ambienti sanitari specificamente progettati. Oggi grazie alla miniaturizzazione ed allo sviluppo delle reti è possibile spostare il DM in stanza di degenza, in un ambulatorio remoto o a casa del paziente. Questo rappresenta un aumento dell'esposizione a rischi Cyber


Care delivery and patient safety
IT Security measures
Patching, vulnerability test
device availability
hardening
Usability, functionality
Security benefits

*Contains Nonbinding Recommendations*

# Postmarket Management of Cybersecurity in Medical Devices

---

# Guidance for Industry and Food and Drug Administration Staff

**Document issued on December 28, 2016.**

**The draft of this document was issued on January 22, 2016.**



# The **5 current threats** identified in healthcare

1. Email Phishing Attacks
2. Ransomware Attacks
3. Loss or Theft of Equipment or Data Internal, Accidental or Intentional Data Loss
4. Attacks Against Connected
5. Medical Devices That May Affect Patient Safety

# phishing

- in media solo il 4% degli individui farà clic su una mail infetta: ma  chi sono quei 4%?
- 32% dei breaches è legato al phishing
- Necessità di fare prevenzione attraverso la formazione



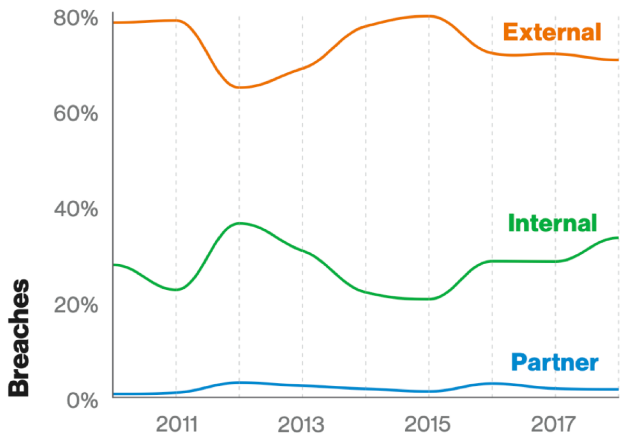



**Figure 6.** Threat actors in breaches over time

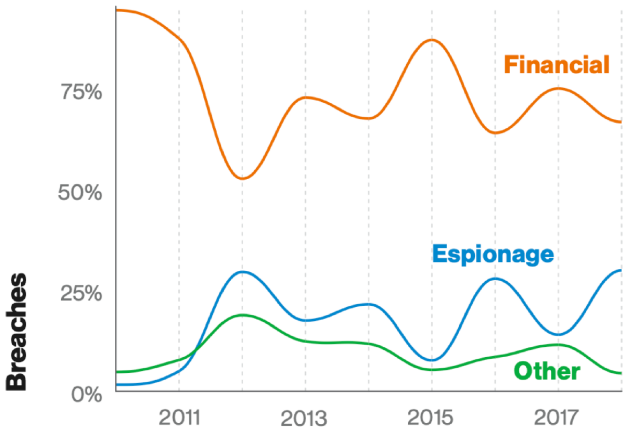



**Figure 7.** Threat actor motives in breaches over time


**Figure 2.** Who are the victims?

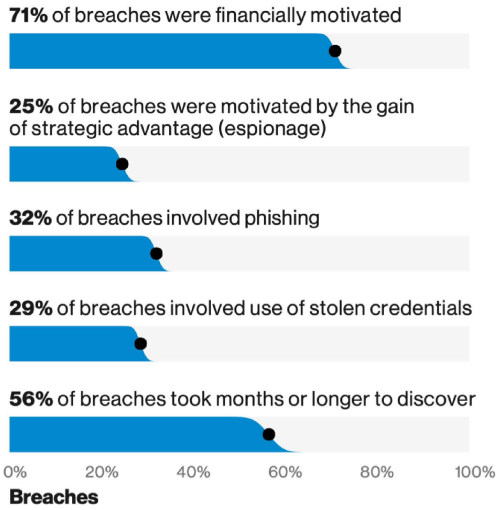
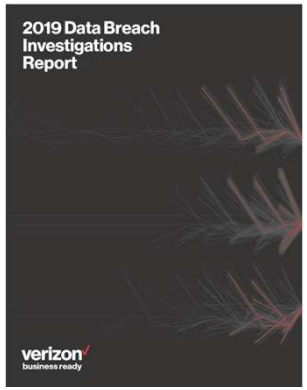



**Figure 5.** What are other commonalities?




Verizon 2019 Data Breach Inves6ga6ons Report (DBIR)

# IL CASO URGENT/11



FDA NEWS RELEASE

# FDA informs patients, providers and manufacturers about potential cybersecurity vulnerabilities for connected medical devices and health care networks that use certain communication software



More Press Announcements

Press Announcements

**For Immediate Release:** October 01, 2019

Today, the U.S. Food and Drug Administration is informing patients, health care professionals, IT staff in health care facilities and manufacturers of a set of cybersecurity vulnerabilities, referred to as "URGENT/11," that—if exploited by a remote attacker—may introduce risks for medical devices and hospital networks. URGENT/11 affects several operating systems that may then impact certain medical devices connected to a communications network, such as wi-fi and public or home Internet, as well as other connected equipment such as routers, connected phones and other critical infrastructure equipment. These cybersecurity vulnerabilities may allow a remote user to take control of a medical device and change its function, cause denial of service, or cause information leaks or logical flaws, which may prevent a device from functioning properly or at all.

To date, the FDA has not received any adverse event reports associated with these vulnerabilities. The public was first informed of these vulnerabilities in a July 2019 advisory sent by the Department of Homeland Security. Today, the FDA is providing additional information regarding the source of these vulnerabilities and recommendations for reducing or avoiding risks the vulnerabilities may pose to certain medical devices.

"While advanced devices can offer safer, more convenient and timely health care delivery, a medical device connected to a communications network could have cybersecurity vulnerabilities that could be exploited resulting in patient harm," said Amy Abernethy,

**Content current as of:**
10/01/2019

**Regulated Product(s)**
Medical Devices

**Follow FDA**
Follow @US_FDA
Follow FDA
Follow @FDAmedia



# Urgent11, le 11 vulnerabilità gravi di 200 milioni di dispositivi connessi

Firewall, router, centralini VoIP, ma anche stampanti di rete e dispositivi di controllo di processi industriali: sono queste le possibili vittime delle vulnerabilità. Le falle presenti in VxWorks, l'RTOS di Wind River presente su oltre 2 miliardi di dispositivi

di Andrea Bai pubblicata il **30 Luglio 2019**, alle **14:22** nel canale SECURITY

Armis, società di sicurezza informatica focalizzata sul mondo Internet of Things, ha oggi rivelato i dettagli di 11 vulnerabilità battezzate, complessivamente, "**Urgent11**", che possono avere impatto su un'ampia gamma di dispositivi: da router a sistemi medicali, passando per stampanti e macchinari industriali. Nello specifico le vulnerabilità affliggono VxWorks, un RTOS (real-time operating system) di Wind River.

Gli RTOS sono semplici sistemi operativi con funzionalità di base che vengono utilizzati per quei dispositivi che hanno accesso ad un numero limitato di risorse, come i chipset dei **dispositivi IoT** dove è necessario gestire solamente operazioni di input/output con poca elaborazione di dati e senza la necessità di un'interfaccia grafica o visuale. VxWorks, in particolare, è un RTOS molto popolare in quanto si trova su oltre due miliardi di dispositivi, secondo quanto dichiarato dalla stessa Wind River.

Come dicevamo le falle sono state rese oggi di pubblico dominio (e verranno presentate approfonditamente in occasione della Black Hat Security Conference di Las Vegas il prossimo 8 agosto), ma **Armis e Wind River hanno collaborato a stretto contatto per risolvere il problema**, con il rilascio delle patch correttive già durante le scorse settimane. Wind River ha inoltre sottolineato che il problema non è ascrivibile esclusivamente al suo RTOS: "Lo stack IPnet è parte di Wind River tramite l'acquisizione di Interpeak nel 2006, in precedenza era usato in licenza da svariati produttori di ROTS".

## Le 11 vulnerabilità Urgent11

https://youtu.be/tpSXr4XhQwM

# Affected Devices

As mentioned above, The URGENT/11 vulnerabilities affect all VxWorks versions since version 6.5, excluding versions of the product designed for certification, such as VxWorks 653 and VxWorks Cert Edition. New updates have been provided and more information can be found in the Wind River Security Alert posted on the company's Security Center.

## A partial list of devices impacted include:

- SCADA devices
- Industrial controllers
- Patient monitors
- MRI machines
- Firewalls
- VOIP phones
- Printers



ARMIS

PLATFORM SOLUTIONS PARTNERS RESOURCE CENTER ABOUT REQUEST A DEMO

## Partial list of companies or devices using VxWorks versions impacted by URGENT/11 (links to company's advisories have been included, if available):

- ABACO Systems
- Alcatel-Lucent
- ABB
- Avaya
- BD
- Belden Industrial Devices
- BR Automation
- Dräger
- Extreme Networks
- GE Healthcare
- Honeywell
- NetApp
- Opto22
- Philips
- Rockwell Automation
- Schneider Electric
- Siemens



## GE Healthcare Guidance on Cyber

| Device | 1. Flow Sensor Scenario | 2. Alarm Silence Scenario | 3. Clock Scenario | 4. Weight and Age Scenario |
|---|---|---|---|---|
| Aespire 7100 / 100 / Protiva / Carestation | Yes[a], Software Version 1.x | Yes | No | No |
| Aestiva 7100 | Yes[b], Software Version 1.x | Yes | No | No |
| Aestiva 7900 | Yes[c], Software Versions 1.x, 2.x, 3.x | Yes | No | No |
| Aestiva MRI | Yes[d], Software Version 3.x | Yes | No | No |
| Aespire 7900 | No | Yes | No | No |
| Aespire View | No | Yes | No | No |
| Aisys, Aisys CS², Avance, Amingo, Avance CS² | No | Yes | Yes | Yes |
| Carestation 620/650/650c | No | Yes | Yes | Yes |

[a] Devices manufactured prior to October 2010.

[b] Devices manufactured prior to February 2014.

[c] Devices manufactured prior to March 2004.

[d] Devices manufactured prior to July 2014.

## Datex Ohmeda Aespire 7900 Anaesthesia machine

# FINE