

AIIC 2023

FORTEZZA DA BASSO

Firenze 10-13 maggio 2023



Convegno Nazionale
Associazione Italiana Ingegneri Clinici

Innovazione e accessibilità:
il governo delle tecnologie sanitarie come sfida sociale



IC



CYBERSECURITY E DISPOSITIVI MEDICI: LA SICUREZZA CHE VERRA'

Maurizio Rizzetto



f.f. DIRETTORE DIPARTIMENTO TECNICO ASFO

MEMBRO COMITATO ICT DI AIIC



MEMBRO COMITATO HIMSS ITALIAN COMMUNITY

USER CO-CHAIR IHE ITALIA



AIIC 2023

FORTEZZA DA BASSO

Firenze 10-13 maggio 2023

Convegno Nazionale
Associazione Italiana Ingegneri Clinici



Innovazione e accessibilità:
il governo delle tecnologie sanitarie come sfida sociale



CYBERSECURITY E DISPOSITIVI MEDICI: LA SICUREZZA CHE VERRA' - CORSO N. 4

Responsabile scientifico: Andrea Gelmetti (*GdL ICT - AIIC*)

Docenti:

Maurizio Rizzetto (*GdL ICT - AIIC*)

Paolo Piaser (*Azienda Sanitaria Friuli Occidentale*)

Andrea Assunto (*CISO Fondazione IRCCS Policlinico San Matteo*)

Programma:

- **13:30 - 14:30** Introduzione e descrizione dello scenario. Il ruolo dell'Ingegnere Clinico nel mondo della Cybersecurity
- **14:30 - 15:45** Il quadro normativo di riferimento ed i principali adempimenti in ambito sanitario
- **15:45 - 16:30** Simulazione - Tabletop Exercise TTE

AIIC 2023

FORTEZZA DA BASSO

Firenze 10-13 maggio 2023

Convegno Nazionale
Associazione Italiana Ingegneri Clinici

Innovazione e accessibilità:

il governo delle tecnologie sanitarie come sfida sociale

Un po' di storia

IC / IT Convergence

CHIME

Convergence of Clinical Engineering and Information Technology

August 24, 2006

Stephen L. Grimes, FACCE SHIMSS
Director, Clinical Engineering
Vanderbilt University Medical Center
Past Chair, Medical Device Security Workgroup
Health Information and Management Systems Society (HIMSS)
President
American College of Clinical Engineering (ACCE)

Trends - Changes in Medical Technology Moving from Discrete Devices to integrated "Systems"

- Medical devices and systems are being designed and operated as special purpose computers ... more features are being automated, increasing amounts of medical data are being collected, analyzed and stored in these devices



- There has been a rapidly growing integration and interconnection of disparate medical (and information) technology devices and systems where medical data is being increasingly exchanged



August 2006

© slg ~ 8

AIIC 2023

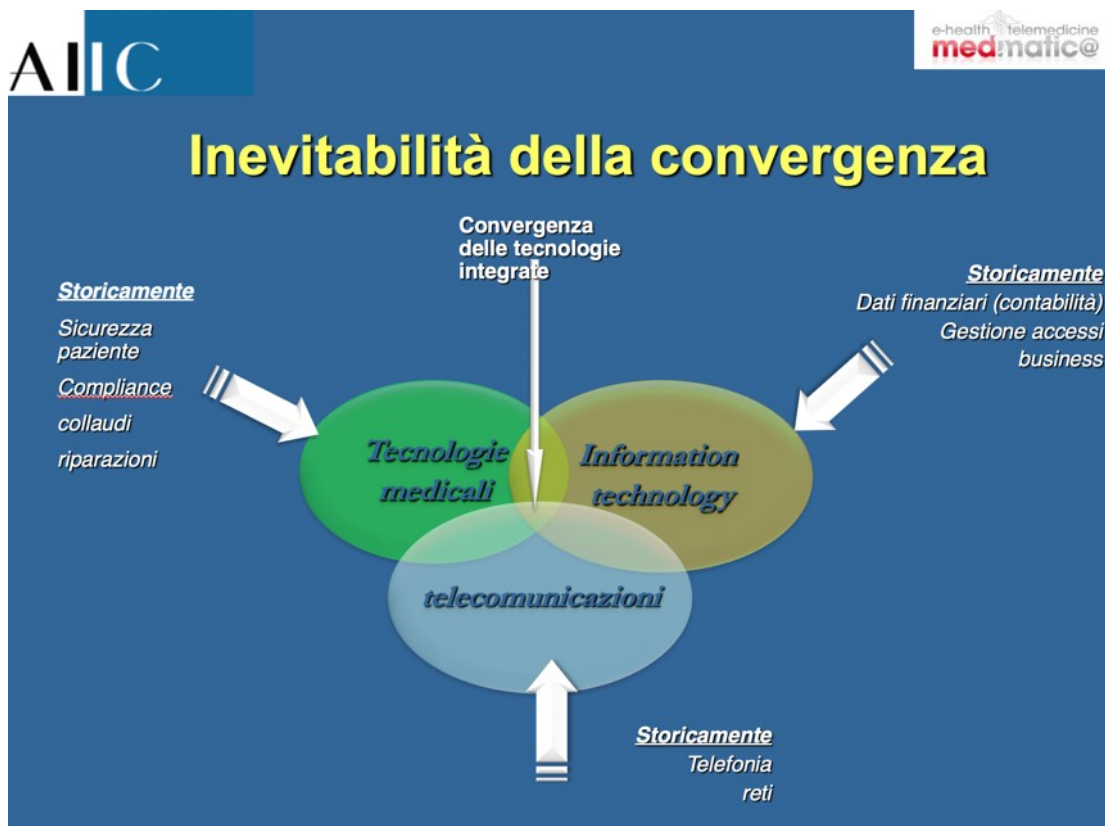
FORTEZZA DA BASSO

Firenze 10-13 maggio 2023

Convegno Nazionale
Associazione Italiana Ingegneri Clinici

Innovazione e accessibilità:
il governo delle tecnologie sanitarie come sfida sociale

medmatic@ Vicenza 2008



AIIC

e-health telemedicine
medmatic@

IHE Patient Care Device Domain IHE PATIENT CARE DEVICE DOMAIN INVITES PARTICIPATION IN DEVELOPING NEW PROFILES

The Patient Care Device Domain (PCD) of Integrating the Healthcare Enterprise International (IHE) develops standards-based *interoperable* communications that involve medical devices and systems, where one or more components are regulated medical devices.

Interoperability provides users and vendors with many benefits:

- Helps reduce medical errors
- Contributes to improved workflow and efficiency, easing the burden on caregivers and providing data where and when needed
- Reduces development and implementation costs
- Meets user demands for the ability to purchase appropriate technologies for differing applications

[\[read more\]](#)



ACCE-HIMSS Excellence in Clinical Engineering and Information Technology Synergies Award 2009

Nominations are now open for the ACCE HIMSS Clinical Engineering Synergies Award. The Award will be presented at the HIMSS 2009 Awards Banquet in Chicago (April 2009), to one or more individuals who has best demonstrated leadership in promoting or implementing significant synergies between the clinical engineering and information technology professions. All Nominations must be submitted by October 30th, 2008

[Award Criteria](#) (.doc, 69Kb) | [Nomination Form](#) (.doc, 36Kb)



[Click here](#) for more information.

ACCE Newsletter

Sept / Oct 2008
Volume 18, Issue 5

- Inside this issue:
- Medical Device Connectivity - IT Convergence
 - ExCEL Award Presented to Dr. Easy in Toronto
 - Benchmarking for Clinical Engineering Departments
 - Peru Embraces Medical Technology Management
 - The Joint Commission Improves its Accreditation Process
 - Election Time and more...

[Newsletter Homepage](#)

Robert L. Morris
1936-2001

AIIC

e-health telemedicine
medmatic@

CE-IT COMMUNITY

A CLINICAL ENGINEERING/IT COLLABORATION

SPONSORED BY:
AAMI ACCE HIMSS

[About CE-IT Community](#) | [Membership Organizations](#) | [News/Events](#) | [How to Get Involved](#)



Welcome to the CE-IT Community

Our three organizations have joined forces to advance the timely and critical issues facing the clinical engineering/IT community.

We represent thousands of biomedical equipment technicians, clinical engineers, IT professionals, clinicians, and other medical technology professionals around the world.

Each of our organizations has established programs, publications, and organizational structures for its membership.

By pooling our resources through this collaboration, we are seeking to: foster a united voice for IT and clinical engineering concerns; and develop important resources, best practices, and networking opportunities to advance the interests of CE-IT issues in healthcare.

WHAT'S NEW

CE-IT Town Hall Meeting
Date & Time: Tuesday, July 15,
2008 1:00pm central/2:00pm
eastern
BeaStar

[Click Here for the Town Hall July 15, 2008 Meeting Materials](#)

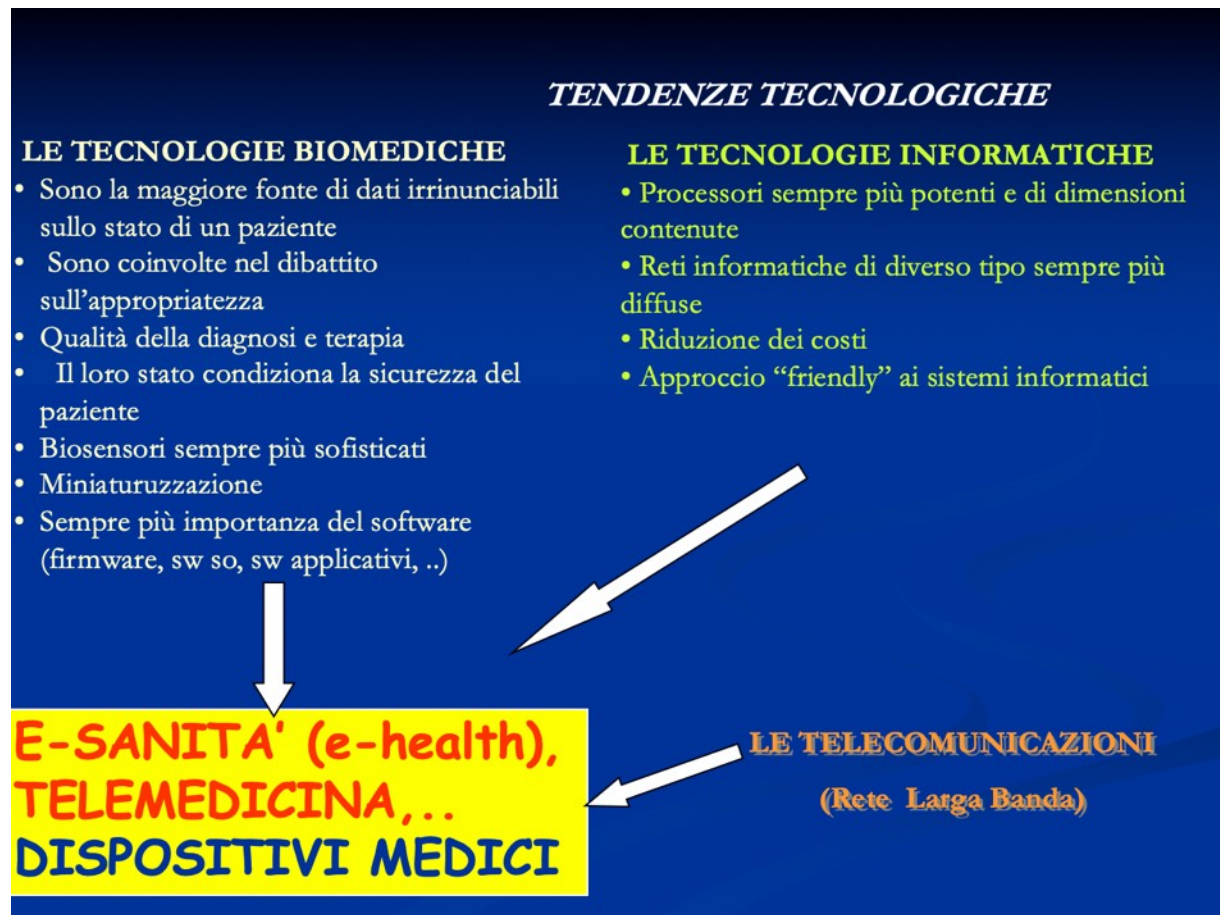
[New Healthcare IT Survey Pinpoints Professional Needs](#)

[View the Survey Results](#)

[New IT Website Launched for Medical Technology Professionals](#)

[Associations Team Up to Advance Clinical Engineering/IT Integration-Feb. 2008](#)

Forum Risk Management, Arezzo 2008



Massimo Garagnani, Vincenzo
Ventimiglia
Forum Risk management, 2008

Why and how to improve EU cyber security

WHY?

The EU works to face cyber threats and challenges, but also to grasp opportunities

CHALLENGES
SOME OF THE MOST CYBER DEPENDENT SECTORS

HEALTH

TRANSPORT

ENERGY

FINANCE

EU countries discuss measures such as:

A STRONGER EU CYBER AGENCY

AN EU-WIDE CYBER SECURITY CERTIFICATION SCHEME FOR PRODUCTS AND SERVICES

AIIC 2023

FORTEZZA DA BASSO

Firenze 10-13 maggio 2023

Convegno Nazionale
Associazione Italiana Ingegneri Clinici

Innovazione e accessibilità:

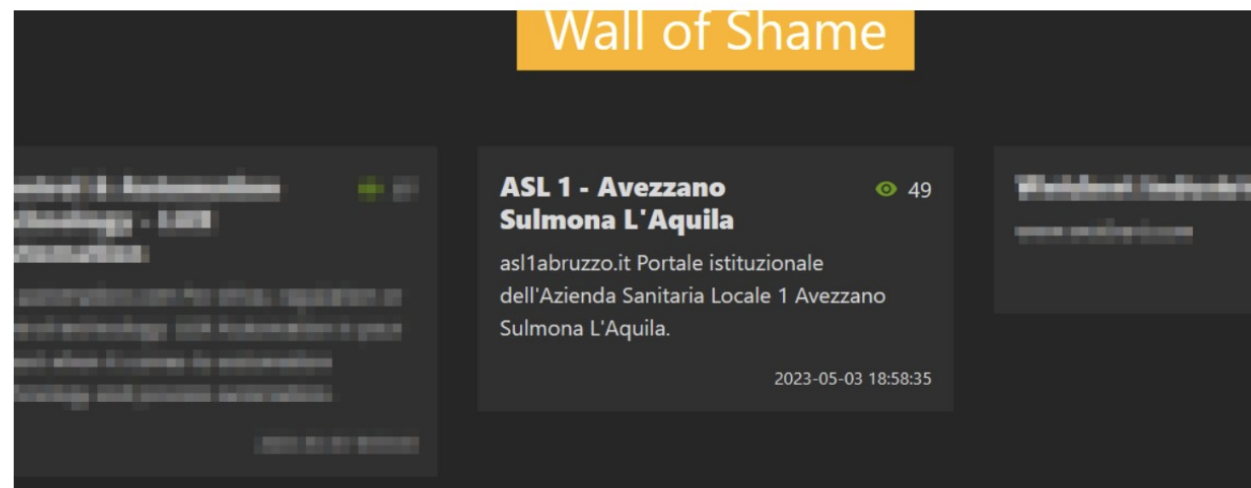
il governo delle tecnologie sanitarie come sfida sociale

Il contesto

ATTACCO HACKER ASL L'AQUILA: E' PIENA EMERGENZA, PRESTAZIONI PARALIZZATE, CHIESTO RISCATTO

6 Maggio 2023 10:19

REGIONE - CRONACA



Tweet

L'AQUILA – Situazione sempre più tesa alla Asl provinciale dell'Aquila, vittima di un micidiale attacco informatico degli hacker che ha messo fuori uso i server e paralizzato servizi sanitari degli ospedali e ambulatori in tutta la provincia, dalla notte del 3 maggio, e ad essere stati trafugati sono stati oltre 500 gigabyte di dati sensibili, tra referti, analisi, cartelle cliniche ed esami.

Italia

Jonathan Greig

May 3rd, 2023

Government

Cybercrime

News



Italian water supplier serving 500,000 people hit with ransomware attack

An Italian company that provides drinking water to nearly half a million people is experiencing some technical disruptions following a ransomware attack.

Alto Calore Servizi SpA runs the collection, supply and distribution of drinking water for 125 municipalities Avellino and Benevento — two provinces in southern Italy. The government-run company also manages sewage and purification services for both provinces.

The company manages 58 million cubic meters of water a year. But on Friday, the company said a recent hack rendered all of their IT systems unusable.

“It will not be possible to carry out any operations or provide information that requires querying the database,” the company said.

“The restoration of the system will be related through press bodies. We apologize for the outage.”



Ospedali

Jonathan Greig

April 14th, 2023

Briefs

Cybercrime



Cyberattack causing treatment delays at Canadian hospital

A cyberattack on a hospital in Ontario, Canada, is causing delays to scheduled and non-urgent care.

Cornwall Community Hospital — a healthcare facility serving the residents of Cornwall and several other counties — said it discovered a “network issue” on Tuesday that was later revealed to be a cyberattack.

The hospital did not respond to requests for comment about whether it was a ransomware attack, but on Thursday officials said it hired cybersecurity experts to respond to the issue.

“At this time, we can confirm that our clinical Electronic Health Record has not been impacted. Delivering exceptional patient-centered care is the hospital’s top priority and CCH continues to provide high-quality clinical services,” the hospital **said** in a statement.

“However, residents may experience some delays to scheduled or non-urgent care.”

The hospital **released** a similar message on Tuesday saying there would be delays in treatment as they deal with the incident.

The organization urged patients to follow its social media channels for more updates on when services may return to normal. The hospital has 175 beds and a staff of 1,200 employees, including 180 physicians

Jonathan Greig

April 24th, 2023

Government

News

Cybercrime

Technology



CISA adds printer bug, Chrome zero-day and ChatGPT issue to exploited vulnerabilities catalog

The Cybersecurity and Infrastructure Security Agency (CISA) added an issue affecting a popular print management software tool to its list of exploited vulnerabilities on Friday.

PaperCut is a software company that produces printing management software for Canon, Epson, Xerox, Brother and almost every other major printer brand. Their tools are widely used within governments agencies, universities, and large companies around the world.

But on Wednesday, the company published an [urgent update to an advisory](#) recommending companies install a patch for the vulnerability.

“We have evidence to suggest that unpatched servers are being exploited in the wild,” the company said. The first published an advisory about the issue on March 8.

Farmaci

Jonathan Greig

April 12th, 2023

Briefs



German drug development company says cyberattack causing production delays

German drug development giant Evotec is still recovering from a cyberattack that forced it to take all of its IT systems offline.

The cyberattack last Thursday prompted them “to secure [their systems] from data corruption or breaches” by disconnecting them from the internet.

“The IT systems are currently being examined and the scope of the impact is being reviewed. Highest diligence will be applied to data integrity,” the company **said** on Friday.

In an **update** on Monday, the company said a forensic examination of its systems is being conducted by cybersecurity experts and others. Evotec has also contacted law enforcement agencies in Germany about the attack.

Evotec has more than 4,200 employees and had revenue of nearly \$700 million in 2021 through its development of drugs to treat Alzheimer's, Huntington's disease and more. The company has long-term drug discovery partnerships with Bristol Myers Squibb, Bayer, Sanofi and several other pharmaceutical giants.

Evotec still has not reconnected its network but said business continuity has been “upheld at all of its global sites.”

Medical Device

James Reddick

March 29th, 2023

Briefs

Technology



FDA can now reject new medical devices over cyber standards

The Food and Drug Administration **affirmed** Wednesday that medical device manufacturers must now prove their products meet certain cybersecurity standards in order to get the agency's approval.

The guidelines were laid out in the omnibus appropriations bill signed into law last December, which authorized the FDA to impose security requirements on manufacturers and allocated \$5 million to the cause. The rules came into effect on Wednesday — 90 days after the bill was enacted.

The rules pertain to all new medical device applications, but regulators said they will work with companies to help them meet standards until October 1.

Under the law, manufacturers must design and release updates and patches after a product goes to market, provide a software bill of materials, and submit a plan for identifying and addressing "postmarket cybersecurity vulnerabilities." The rules impact devices that have software and are connected to the internet, for example insulin pumps, blood sugar monitors, and certain pacemakers.

"The medical device industry has never had so many products connected to the internet," said Tiffany Gallagher, health industries risk & regulatory leader at PwC. "As innovations in healthcare technology continue to grow, these regulations will help ensure that cybersecurity is baked into devices from the very beginning and continues to be a top-of-mind priority beyond the initial implementation."

Crisi Mondiali

Jonathan Greig
March 19th, 2023

Government

Nation-state

Briefs

Cybercrime



Pro-Russia hackers are increasingly targeting hospitals, researchers warn

Cybersecurity researchers said this week that they have observed the pro-Russia hacking group known as Killnet increasingly launch distributed denial of service (DDoS) attacks targeting healthcare organizations since November.

Killnet was established following Russia's invasion of Ukraine in February 2022, and spent most of the last year launching DDoS attacks against **governments and companies** around the world.

While the attacks are mostly a nuisance – knocking websites offline for about an hour in most cases – they have caused concern within the U.S. government, particularly when they are launched at critical infrastructure like **airports and hospitals**.

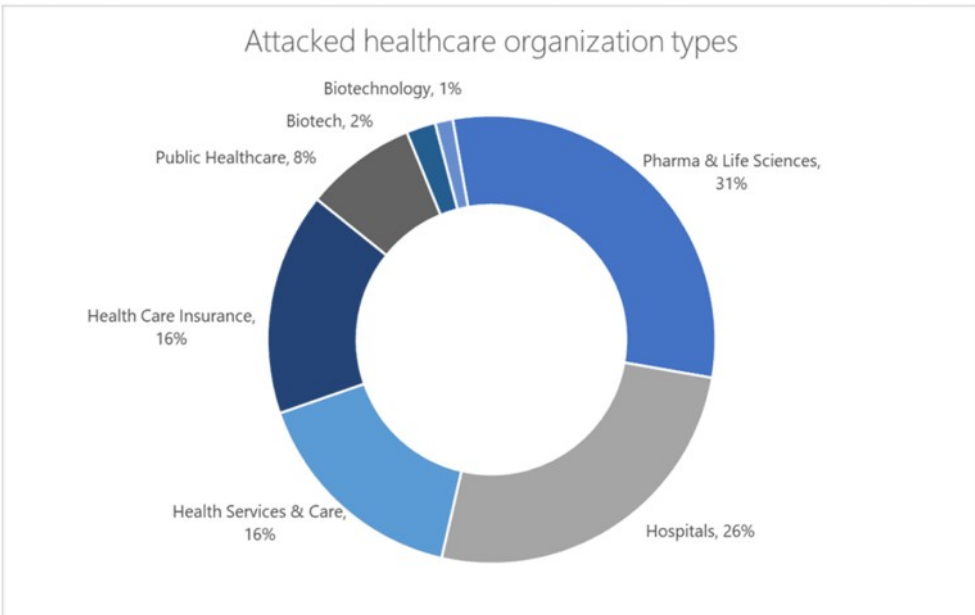


Image: Microsoft

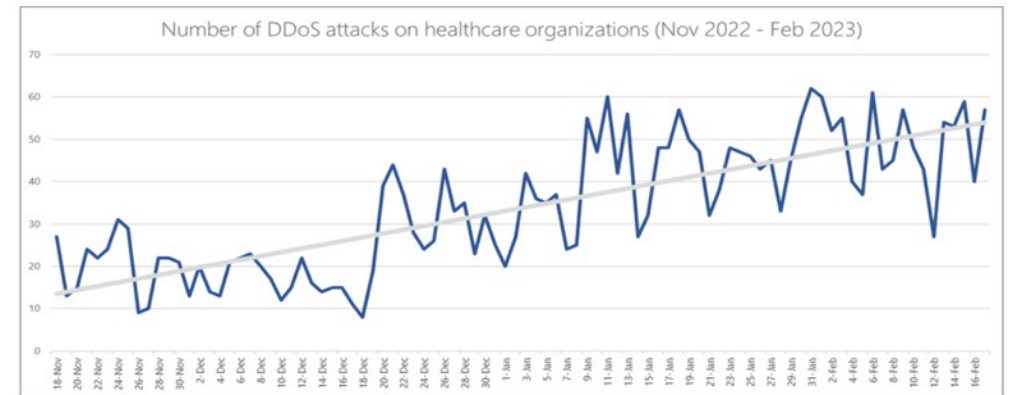


Image: Microsoft

Previsioni Future

The CISA Director's comments come days after Italy's data protection agency [temporarily banned ChatGPT](#), alleging the powerful artificial intelligence tool has been illegally collecting users' data and failing to protect minors.

Italian officials also invoked [a data breach on March 20](#) in which the payment information of ChatGPT subscribers was leaked, as well as some chat records. On Monday, Germany's data protection commissioner told [a local news outlet](#) that they were considering a similar ban due to data security concerns.

Several other European countries [are mulling action](#).

"[AI is] the most powerful technology capability and maybe weapon of this century. We do not have the legal regimes or the regulatory regimes to be able to implement them safely and effectively. And we need to figure that out in the very near term."

Jonathan Greig

April 6th, 2023

News



CISA director: AI cyber threats the 'biggest issue we're going to deal with this century'

A top U.S. cyber official expressed grave concerns about the security implications of generative artificial intelligence at a forum on Thursday, warning that legislative action is needed to regulate its use.

Cybersecurity and Infrastructure Security Agency Director Jen Easterly called popular AI tools like ChatGPT "the biggest issue that we're going to deal with this century" due to the variety of ways they can be used by cybercriminals and nation states.

Last year, the tool from Microsoft-backed OpenAI kicked off an artificial intelligence arms race among the biggest tech companies. Regulators have been struggling to keep up ever since.

The European Union police force Europol [last week warned](#) about how chatbots like ChatGPT could be used for phishing attempts, the spread of disinformation and cybercrime.

"If you think about the most powerful weapon of the last century, it was nuclear weapons. They were controlled by governments and there was no incentive to use them. There was a disincentive to use them," Easterly [told an audience at the Atlantic Council](#).

"[AI is] the most powerful technology capability and maybe weapon of this century. We do not have the legal regimes or the regulatory regimes to be able to implement them safely and effectively. And we need to figure that out in the very near term."

Intelligenza Artificiale

James Reddick

March 31st, 2023

Briefs

Government

Technology

Privacy



ChatGPT privacy and safety concerns lead to temporary ban in Italy

Italy's data protection agency has temporarily banned ChatGPT, alleging the powerful artificial intelligence tool has been illegally collecting users' data and failing to protect minors.

In a provision released Thursday, the agency wrote that OpenAI, the company that owns the chatbot, does not alert users that it is collecting their data.

They also contend that the application lacks age verification, which "exposes children to receiving responses that are absolutely inappropriate to their age and awareness, even though the service is allegedly addressed to users aged above 13."

Failures to notify users of data collection, as well as to justify the hoovering of information, would run afoul of the European Union's [General Data Protection Regulation](#), raising the possibility that other countries in the bloc may follow suit in cracking down on the program.

OpenAI has 20 days to address the allegations, and either remedy or justify them. Otherwise, it could face a fine of up to 20 million euros (\$21.7 million).

The agency's press statement also invoked a [data breach on March 20](#) in which the payment information of ChatGPT subscribers was leaked, as well as some chat records.

OpenAI did not respond to The Record's request for comment.

The announcement from the Italian government follows the [release of a letter](#) endorsed by more than 1,000 technology leaders calling for a temporary moratorium on development of artificial intelligence beyond GPT-4, the most

TITOLO SLIDE

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Inserire il testo o il doc web

CERCA



I miei diritti



Imprese ed enti

L'Autorità ▾

Temi ▾

Normativa e provvedimenti ▾

News e comunicazione ▾

Amministrazione trasparente

[Home](#) / [Stampa e comunicazione](#) / [Comunicato stampa](#)[Intelligenza artificiale: il Garante blocca ChatGPT. Raccolta illecita di dati personali. Assenza di sistemi per la verifica dell'età dei minori](#)

Intelligenza artificiale: il Garante blocca ChatGPT. Raccolta illecita di dati personali. Assenza di sistemi per la verifica dell'età dei minori

Scheda

Doc-Web
9870847Data
31/03/23

TITOLO SLIDE



GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Inserire il testo o il doc web

CERCA



I miei diritti



Imprese ed enti

L'Autorità



Temi



Normativa e provvedimenti



News e comunicazione



Amministrazione trasparente

Home / Stampa e comunicazione / Comunicato stampa

/ ChatGPT: OpenAI riapre la piattaforma in Italia garantendo più trasparenza e più diritti a utenti e non utenti europei

ChatGPT: OpenAI riapre la piattaforma in Italia garantendo più trasparenza e più diritti a utenti e non utenti europei

Scheda



Doc-Web
9881490

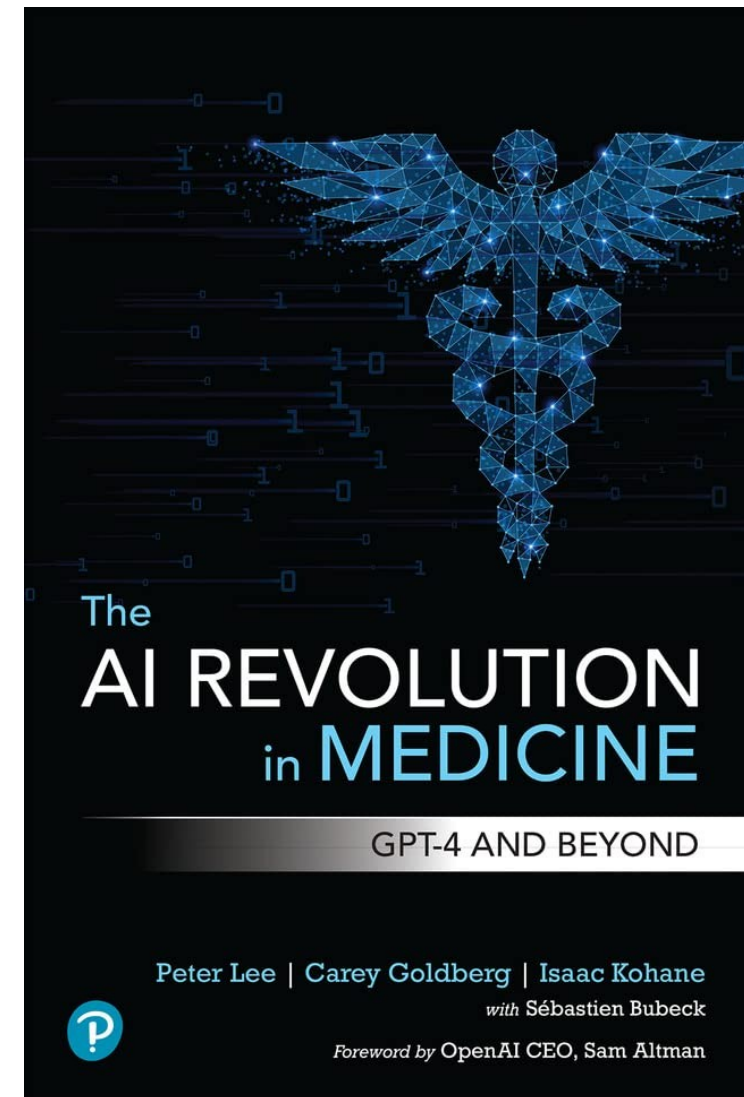
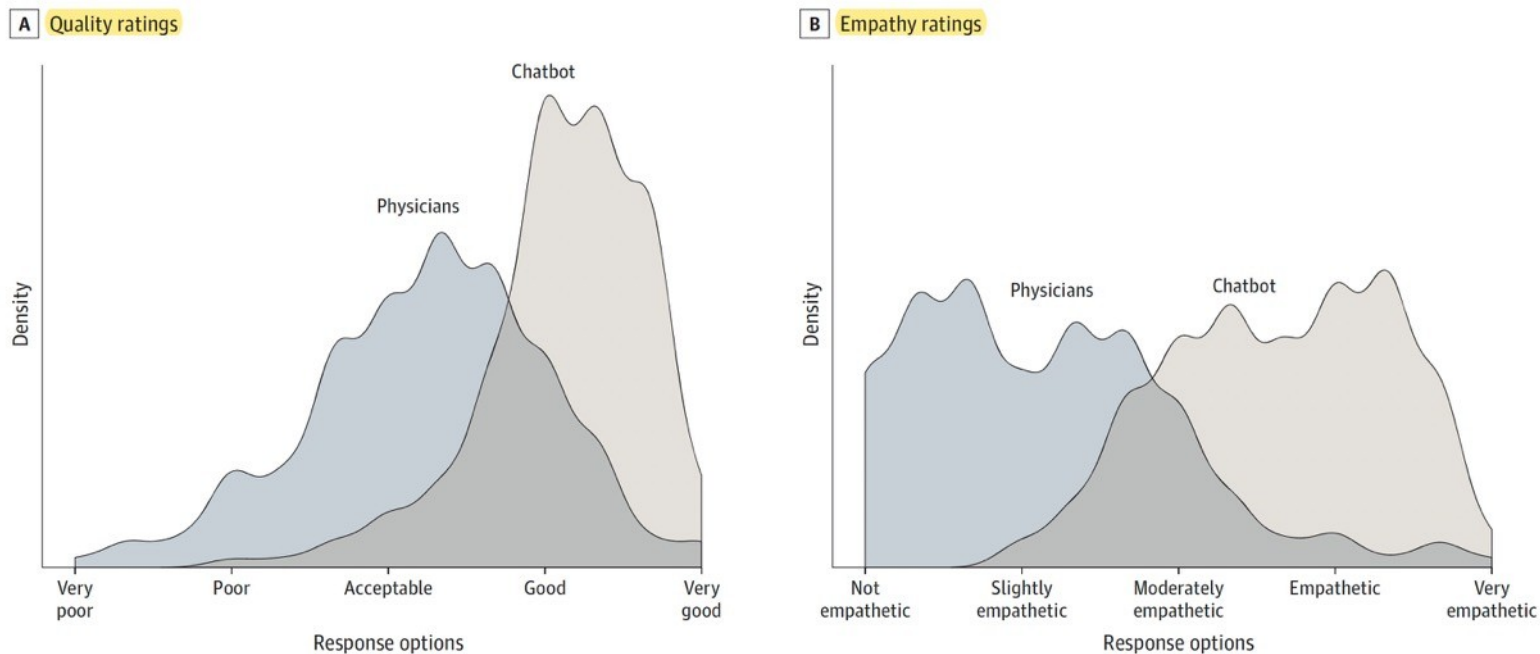


Data

When Patient Questions Are Answered With Higher Quality and Empathy by ChatGPT than Physicians

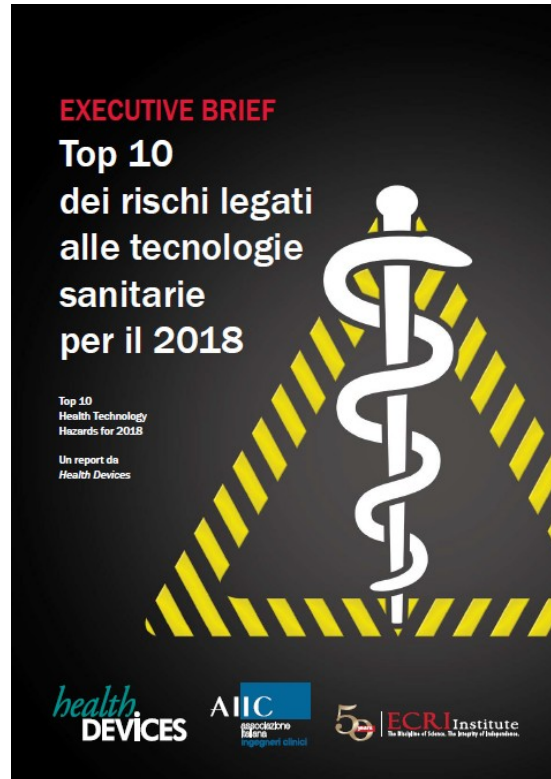
Eric Topol 28 apr 2023

Figure. Distribution of Average Quality and Empathy Ratings for Chatbot and Physician Responses to Patient Questions





Gestione in sicurezza delle tecnologie



1. I ransomware ed altre **minacce informatiche** possono mettere in pericolo i pazienti
2. Il reprocessing inefficace degli **endoscopi** continua ad esporre i pazienti al **rischio di infezioni**
3. **Materassi e fodere** possono essere infettati da fluidi corporei e **contaminanti microbiologici**
4. La configurazione inappropriata di dispositivi e sistemi di notifica secondaria può portare a non rilevare gli **allarmi**
5. Una **pulizia inadeguata** può causare malfunzionamenti dei dispositivi, guasti alle apparecchiature e rischi di lesioni ai pazienti
6. **Elettrodi elettrochirurgici** non correttamente riposti possono causare **ustioni ai pazienti**
7. L'uso inadeguato degli strumenti di imaging digitale può portare all'**esposizione a radiazioni non necessarie**
8. Pratiche non sicure possono vanificare i vantaggi di sicurezza dei sistemi di **amministrazione dei farmaci con codice a barre**
9. **Errori nell'interconnessione di dispositivi medici** possono portare a **cure ritardate o inappropriate**
10. La lentezza nell'adozione di **connettori più sicuri per l'alimentazione enterale** lascia a rischio i pazienti

The List for 2019



ECRI Institute

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*



2019 Top 10

Health Technology Hazards

A Report from Health Devices



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



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 troubleshooting 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 cybersecurity 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.

SEVEN

7

Top 10 Health Technology Hazards for 2021



Executive Brief

ECRI is providing this abridged version of its 2021 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's step-by-step recommendations for addressing the hazards—is available to members of ECRI programs through their membership web pages.

The List for 2021

1. Complexity of Managing Medical Devices with COVID-19 Emergency Use Authorization
2. Fatal Medication Errors Can Result When Drug Entry Fields Populate after Only a Few Letters
3. Rapid Adoption of Telehealth Technologies Can Leave Patients and Data at Risk
4. Imported N95-Style Masks May Fail to Protect Healthcare Workers from Infectious Respiratory Diseases
5. Relying on Consumer-Grade Products Can Lead to Inappropriate Healthcare Decisions
6. Hasty Deployment of UV Disinfection Devices Can Reduce Effectiveness and Increase Exposure Risks
7. Vulnerabilities in Third-Party Software Components Present Cybersecurity Challenges
8. Artificial Intelligence Applications for Diagnostic Imaging May Misrepresent Certain Patient Populations
9. Remote Operation of Medical Devices Designed for Bedside Use Introduces Insidious Risks
10. Insufficient Quality Assurance of 3D-Printed Patient-Specific Medical Devices May Harm Patients



For information about becoming a member of one of our programs, contact clientservices@ecri.org or call +1 (610) 825-6000, ext. 5891.



Top 10 Health Technology Hazards for 2022



Executive Brief

ECRI is providing this abridged version of its 2022 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’s step-by-step recommendations for addressing the hazards—is available to members of ECRI programs through their membership web pages.

The List for 2022

1. Cybersecurity Attacks Can Disrupt Healthcare Delivery, Impacting Patient Safety
2. Supply Chain Shortfalls Pose Risks to Patient Care
3. Damaged Infusion Pumps Can Cause Medication Errors
4. Inadequate Emergency Stockpiles Could Disrupt Patient Care during a Public Health Emergency
5. Telehealth Workflow and Human Factors Shortcomings Can Cause Poor Outcomes
6. Failure to Adhere to Syringe Pump Best Practices Can Lead to Dangerous Medication Delivery Errors
7. AI-Based Reconstruction Can Distort Images, Threatening Diagnostic Outcomes
8. Poor Duodenoscope Reprocessing Ergonomics and Workflows Put Healthcare Workers and Patients at Risk
9. Disposable Gowns with Insufficient Barrier Protection Put Wearers at Risk
10. Wi-Fi Dropouts and Dead Zones Can Lead to Patient Care Delays, Injuries, and Deaths

For information about becoming a member of one of our programs and accessing the full report, contact clientservices@ecri.org or call +1 (610) 825-6000, ext. 5891.

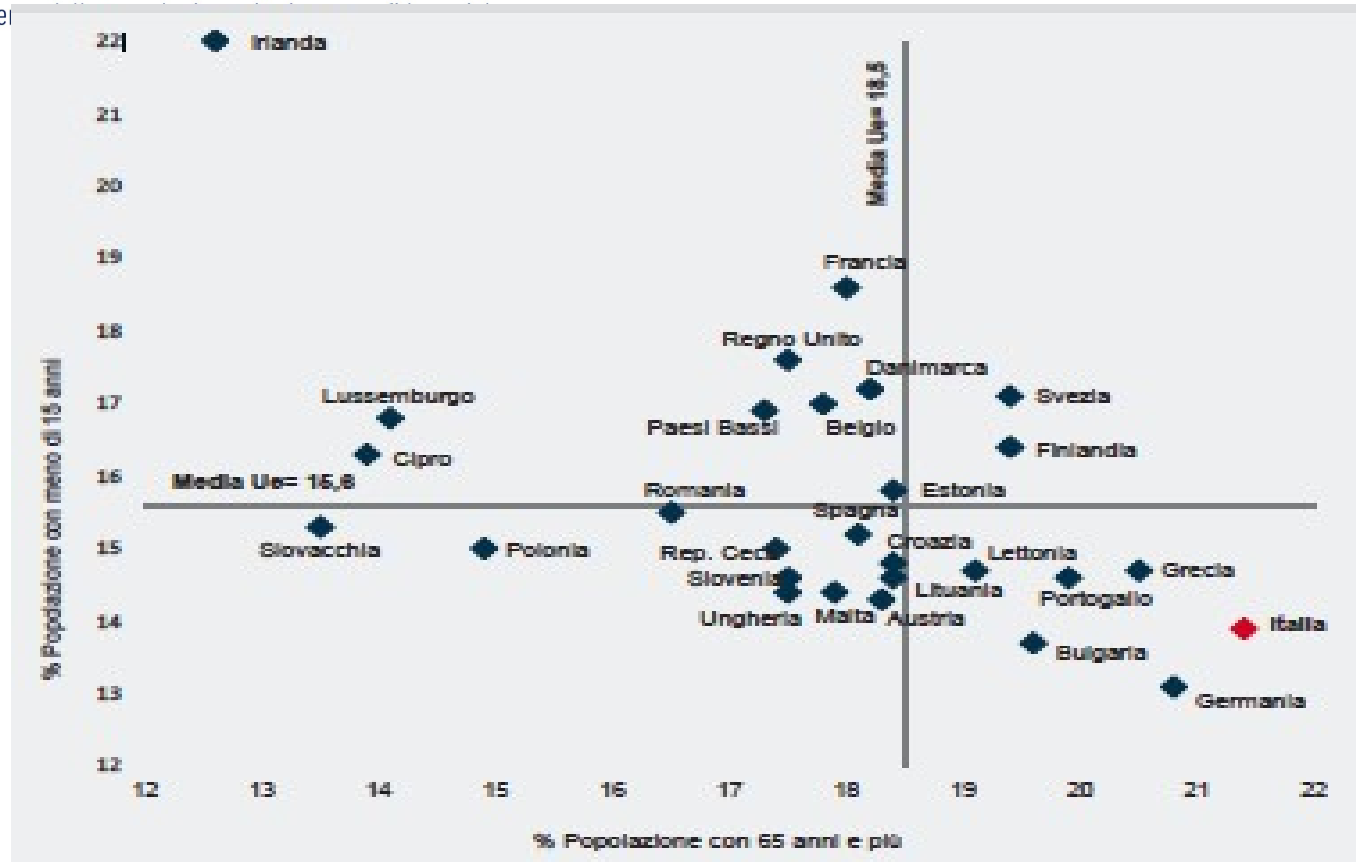
Top 10 Health Technology Hazards for 2023



The List for 2023

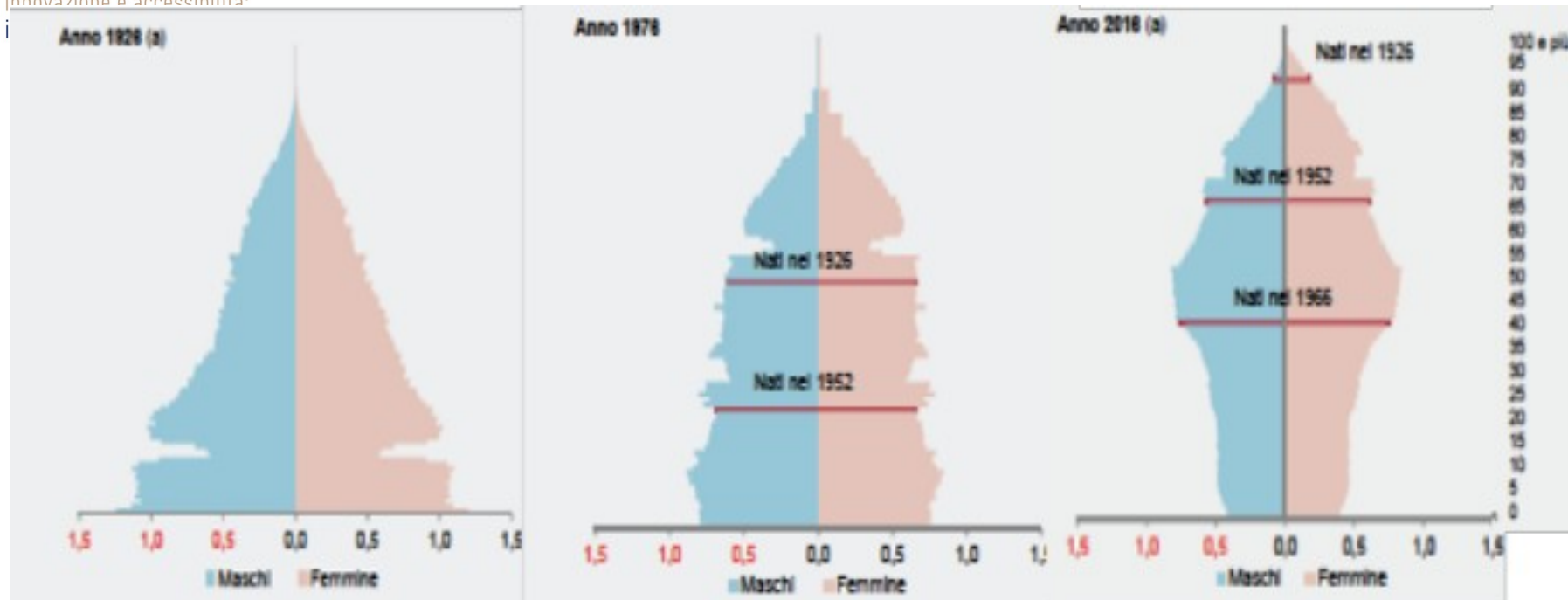
1. Gaps in Recalls for At-Home Medical Devices Cause Patient Confusion and Harm
2. Growing Number of Defective Single-Use Medical Devices Puts Patients at Risk
3. Inappropriate Use of Automated Dispensing Cabinet Overrides Can Result in Medication Errors
4. Undetected Venous Needle Dislodgement or Access-Bloodline Separation during Hemodialysis Can Lead to Death
5. Failure to Manage Cybersecurity Risks Associated with Cloud-Based Clinical Systems Can Result in Care Disruptions
6. Inflatable Pressure Infusers Can Deliver Fatal Air Emboli from IV Solution Bags
7. Confusion Surrounding Ventilator Cleaning and Disinfection Requirements Can Lead to Cross-Contamination
8. Common Misconceptions about Electrosurgery Can Lead to Serious Burns
9. Overuse of Cardiac Telemetry Can Lead to Clinician Cognitive Overload and Missed Critical Events
10. Underreporting Device-Related Issues May Risk Recurrence

Scenario socio-sanitario: come cambia la sanità



*La simultanea presenza di una elevata quota di persone di 65 anni e oltre e di una bassa quota di popolazione al di sotto dei 15 anni colloca il nostro Paese tra i paesi più vecchi del mondo, insieme a Giappone. Sostanzialmente **la popolazione residente decresce e invecchia***

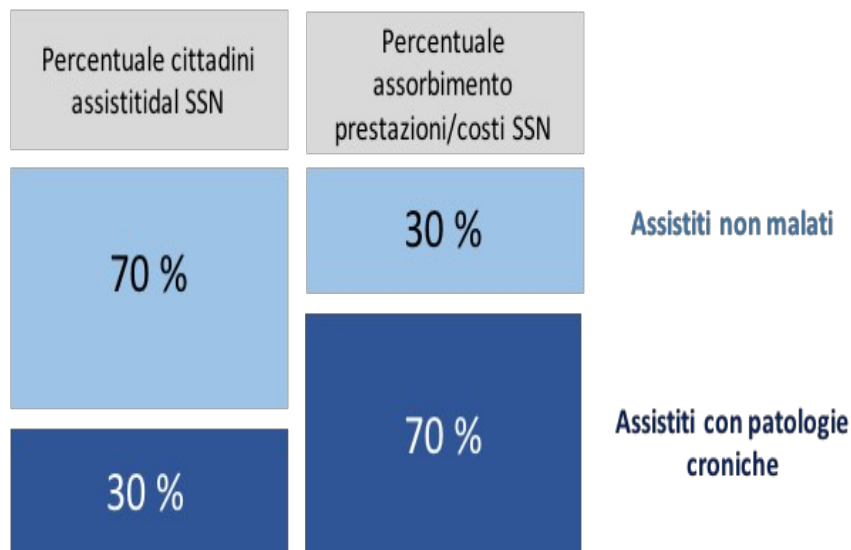
Scenario socio-sanitario: come cambia la sanità



*Le previsioni relative all'evoluzione della struttura demografica della popolazione residente in Italia, elaborate dall'ISTAT, evidenziano che il fenomeno dell'invecchiamento della popolazione nei prossimi decenni assumerà una dimensione particolarmente significativa: tra il 2001 e il 2051 il numero di persone con età pari o superiore ai 65 anni passerà da **10,56 milioni a 17,8 milioni**. E' interessante inoltre considerare il fenomeno degli **over 80 che passerà dagli attuali 1,9ml a 2,9 ml***

Fonte: ISTAT, "Previsioni della popolazione 2001-2051"

Scenario socio-sanitario: come cambia la sanità



Fonte: ri-Elaborazioni dati Istat previsioni 2011-2055; Osservatorio Oasi-UniBocconi

Gli assistiti con **patologie croniche**, pari al **30%** della popolazione, **assorbono oltre il 70%** dei costi del SSN.

L'invecchiamento della popolazione rappresenta uno dei **principali fattori di aumento dell'incidenza di malattie croniche**.

La WHO include infatti l'invecchiamento tra i principali fattori di rischio non modificabili per lo sviluppo delle malattie croniche.

ISTAT prevede che la popolazione over 65, pari al 21,7% nel 2015, passerà nel 2065 al 32,6% con una ulteriore incidenza delle patologie croniche multifattoriali.

Secondo alcune stime nel 2020 le patologie croniche rappresenteranno **il 16% di tutte le patologie nel mondo**.

Il fenomeno delle **malattie croniche multifattoriali** e **delle patologie croniche** è legato non soltanto all'invecchiamento ma anche all'adozione di **stili di vita non salutari** (si stima che il 23% degli italiani sopra i 20 anni sia obeso e che il 33% non svolga attività fisica)

Fonti:

World Health Organisation, Chronic Diseases and their Common Risk Factor, 2005

ISTAT, Previsioni - Anni 2011-2065 - su dati pre-Censimento 2011: indicatori demografici

Trasformazione digitale della sanità: web2.0 e social media



Tra il 2011 e il 2017, la percentuale di utilizzatori del web nella fascia 65-74 anni è passata dal **13,8% al 30,8%**, mentre nella fascia 75+ l'aumento è stato dal 2,7% al 8,8% (ISTAT, 2017).

La “domanda” di tecnologia sta crescendo in ragione dei cambiamenti che avvengono nello scenario del settore, dove altre trasformazioni spingono verso l'individuazione di nuove soluzioni e nuove modalità di risposta ai bisogni dei cittadini over 65.

Fonte: Osservatorio Long Term care. CeRGAS Bocconi 2018

Generation Map

	1946-1964 Baby Boomers Age 54-72	1965-1979 Generation X Age 39-53	1980-1994 Millennials Age 24-38	1995-2009 Generation Z Age 9-23
Social markers	Post-war boom, sexual revolution, rock & roll	Berlin Wall, Black Monday, Thatcherism/ Reagan	New Millennium, 9/11	Global financial crisis, Obama, WikiLeaks
Aspiration	Job security	Work-life balance	Freedom & flexibility	Security & stability
Iconic technology	Digital acquirers TV(56), Audio Cassette (62)	Digital immigrants VCR(76), IBM (81)	Digital natives Internet, SMS, DVD (95)	Technoholics MacBook, iPad, Google
Communication media	Formal Letter	Telephone	SMS/ Email	Social Media
Slanguage	Groovy, Split, Cool, Daddy-O	Dude, Right on!, Wicked, Pschye!	My bad, Wassup?, Phat, Bling	Cray cray, Slay, Bae, YOLO
Music	Audio cassette Elvis, Beatles, Rolling Stones	Walkman/ Boombox Nirvana, Madonna	CD player/iPod Eminem, Britney Spears	Spotify Justin Bieber, Taylor Swift
Family values & situations	Strong family values, multi-child families	First latch-key children, increased divorce rates	Single-parented children	Single or same sex parents
Workforce values	Strong work ethic, loyal to job, strong group workforce	Increasing female workforce, more individually focused	Seek good/work life balance, strong sense of entitlement	Multitaskers, entrepreneurial, seek flexibility
Marketing	Broadcast (mass)	Direct (targeted)	Online (linked)	Digital (social)

Source: Barclays Wealth (2013), Big Arrow Group – *Connect at any age*, Mccrindle (2017)

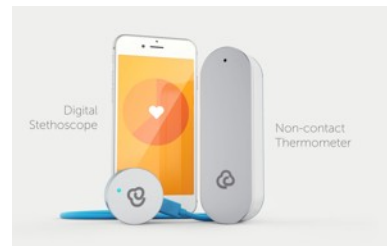
Global and local impact Systems and Device

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



Interoperabilità e medicina di precisione

- Assistenza basata sull'evidenza personalizzata per l'individuo.
“Per me”
- Incoraggiare l'impegno attivo e la partecipazione dei pazienti
- Incoraggiare l'uso delle tecnologie digitali
come “estensori clinici”

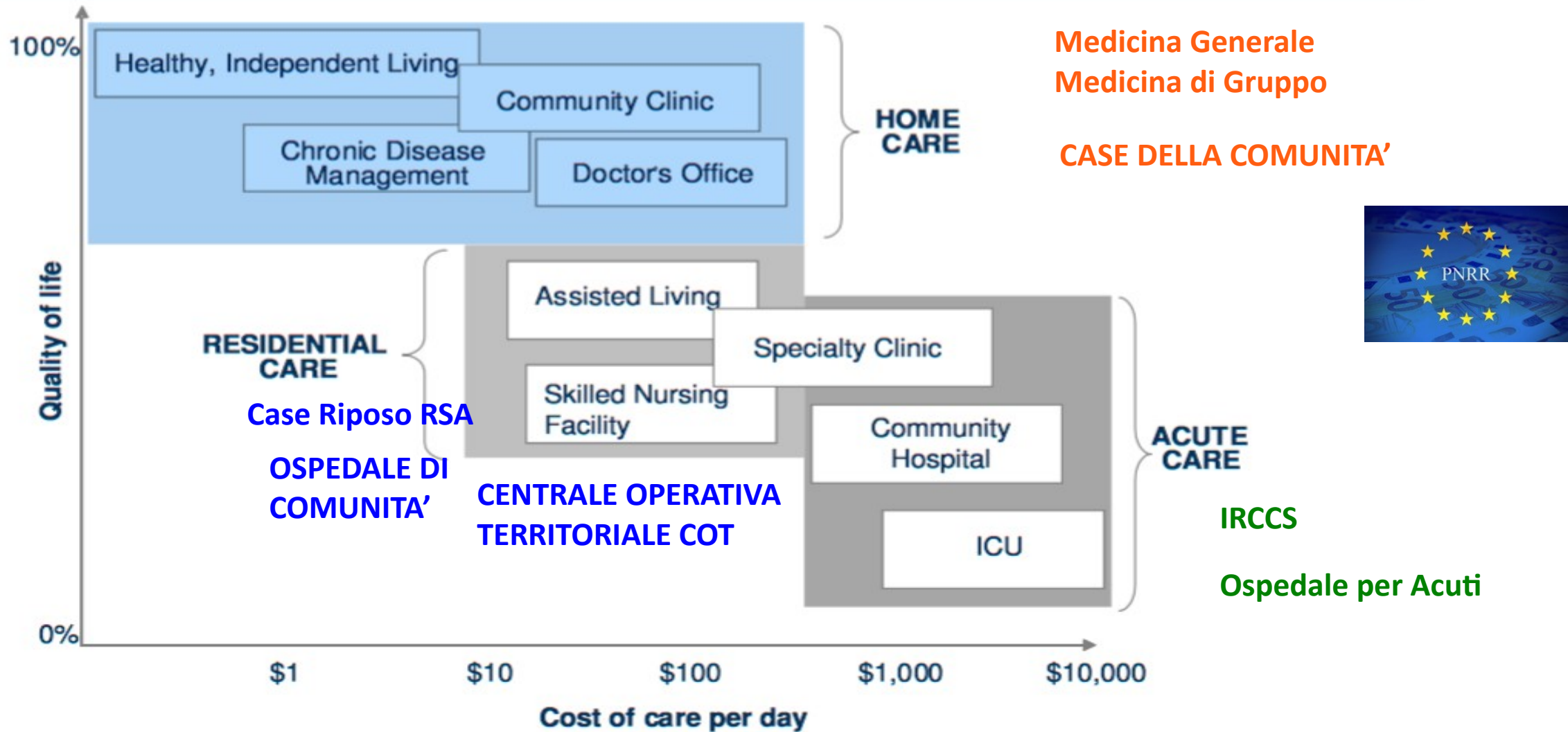


- Approcci predittivi – Genomica
- IOT - Mobile HEALTH

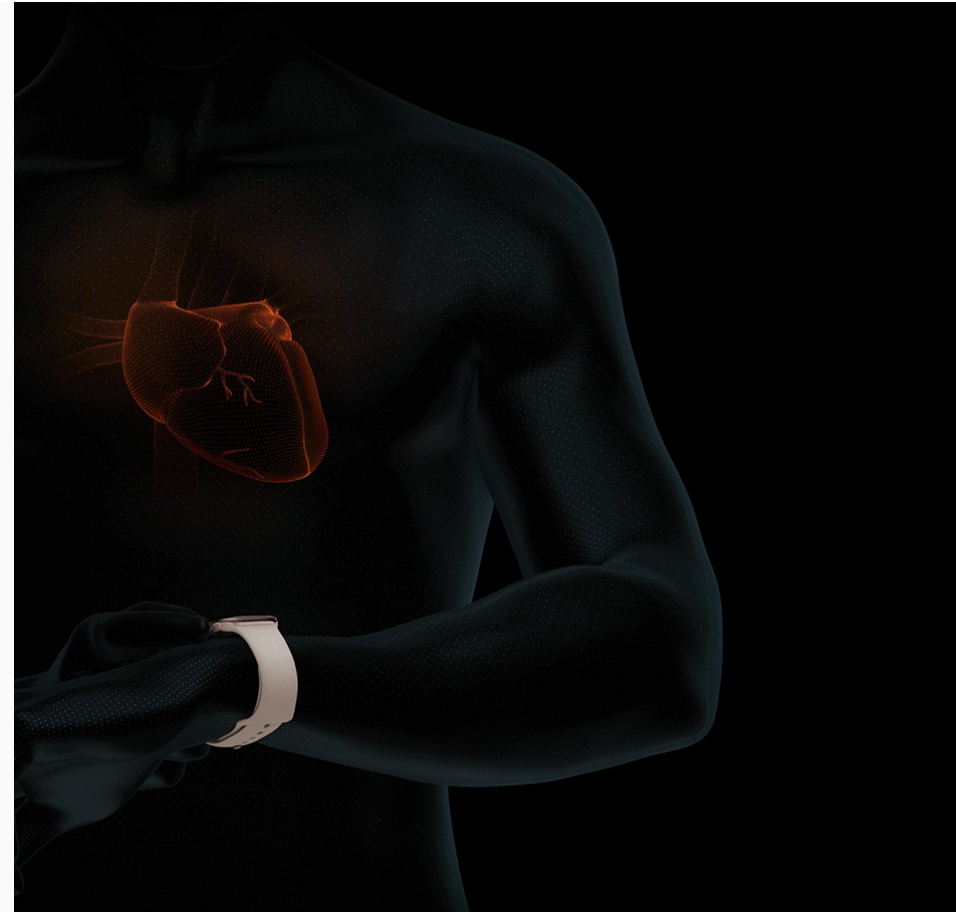
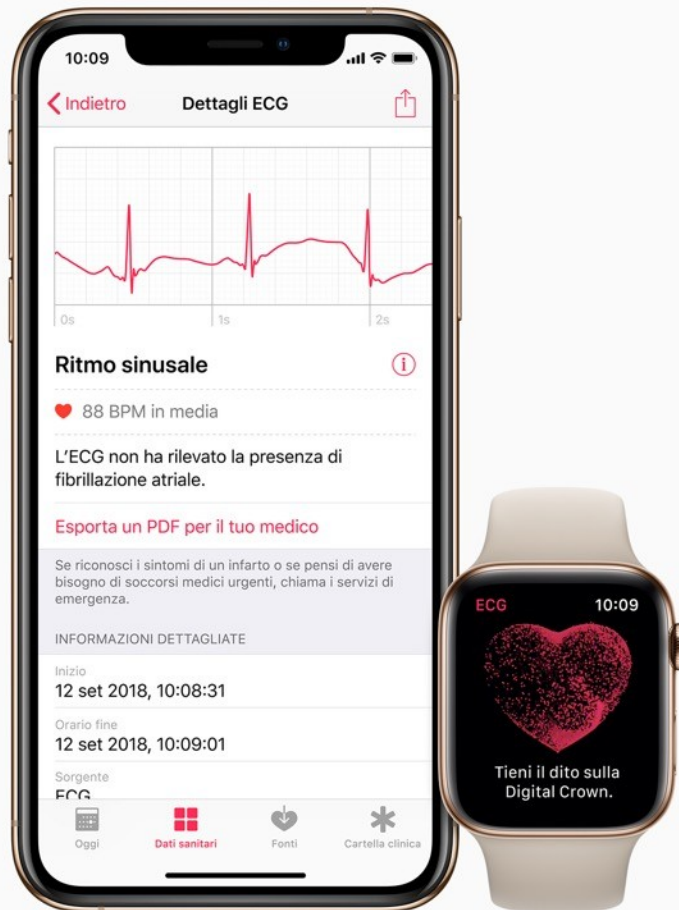


- Implementazione di soluzioni di intelligenza artificiale su larga scala
- Sviluppare e utilizzare registri che aiutino i medici a ridurre le variazioni ingiustificate

Care Delivery will be provided in or near the home



Wearable vs Medical device



Wearable Medical devices



Non invasive measure Press



Omron HeartGuide™ (FDA 2018)



Kardia band

FDA-cleared and CE mark



Butterfly iQ

FDA 510(k) cleared for diagnostic imaging across 13 clinical applications which span the whole body:

- Abdominal
- Cardiac Adult
- Cardiac Pediatric
- Fetal/Obstetric
- Gynecological
- Musculo-Skeletal (Conventional)
- Musculo-Skeletal (Superficial)
- Pediatric
- Peripheral Vessel
- Procedural Guidance
- Small Organ
- Urology

THE WORLD'S FIRST SMARTPHONE-COMPATIBLE ICM

Providing patients with an easy-to-manage heart monitor just got smarter. The Confirm Rx™ ICM offers convenient, connected and continuous monitoring for insight into your patients' conditions, including syncope, palpitations, and AF before or after ablation therapy and cryptogenic stroke—with fewer interruptions to their daily lives and reduced burden to your clinic.

“**THE CONFIRM RX™ ICM WITH THE MYMERLIN™ MOBILE APP ENGAGES PATIENTS WITH EASY-TO-USE TOOLS AND IMPROVES REMOTE MONITORING COMPLIANCE—AND IT IS ONLY FROM ST. JUDE MEDICAL.**”

The Confirm Rx™ ICM is the world's first insertable cardiac monitor that combines a quick and minimally invasive procedure with Bluetooth® low-energy wireless technology, allowing patients to connect using their own mobile devices.

EMPOWER AND ENGAGE PATIENTS

- An all-in-one integrated transmitter and symptom recorder, functional via the myMerlin™ smartphone app, eliminates the need for a traditional radio-frequency (RF) based bedside transmitter, which can be intrusive and cumbersome for patients and limits their mobility.
- The app automatically connects with the device via Bluetooth® low-energy wireless technology, and informs patients of successful device checks and clinic-scheduled transmissions, without interrupting their daily lives.



- **Limitations:** Patients **may use** their own Apple[‡] or Android[‡] mobile device to transmit information from their Confirm Rx™ ICM using the myMerlin™ mobile app. To do so, the device must be powered on, app must be installed, Bluetooth® wireless technology enabled and data coverage (cellular or Wi-Fi[‡]) available. The myMerlin™ app provides periodic patient monitoring based on clinician-configured settings. Transmission data is resent if not sent successfully. **However, there are many internal and external factors that can hinder, delay or prevent acquisition and delivery of ICM and patient information as intended by the clinician.** These factors include: patient environment, data services, mobile device operating system and settings, ICM memory capacity, clinic

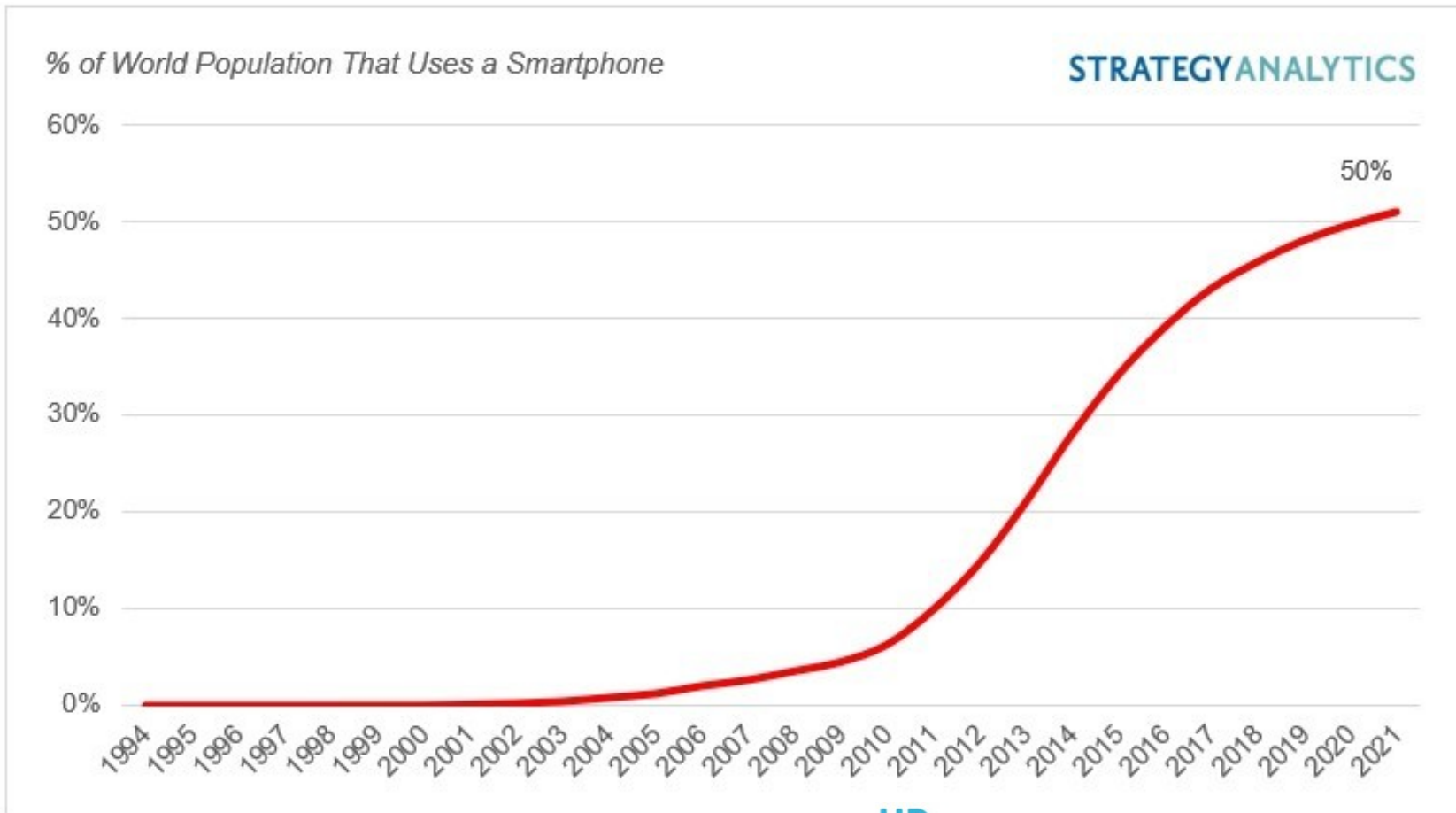
325,000 mHEALTH APPS AVAILABLE – GOOGLE PLAY STORE IS NOW NUMBER ONE FOR HEALTHCARE APPS, OVERTAKING APPLE APP STORE

Number of mHealth apps displayed in App Stores



- 2 Miliardi di persone possiedono uno smartphone
- 50% degli adulti a livello globale
- Oltre il 50% dei possessori di smartphone accede alle informazioni relative alla salute tramite questo dispositivo, circa il **20% ha scaricato una app correlata alla salute**

Smartphone: al mondo sono 4 miliardi, uno ogni due persone



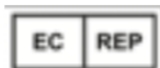
Il Simon è considerato il primo smartphone della storia 1994

App ECG

Istruzioni per l'uso



Apple Inc.
One Apple Park Way
Cupertino, CA 95014
www.apple.com



Apple Distribution International
Hollyhill Industrial Estate,
Hollyhill, Cork,
Ireland
Contatta: medicalcompliance@group.apple.com



Indicazioni di utilizzo

L'app ECG è un'applicazione medica mobile solo software destinata all'utilizzo con Apple Watch per creare, registrare, archiviare, trasferire e mostrare un elettrocardiogramma a canale singolo simile a un elettrocardiogramma a singola derivazione. L'app ECG determina la presenza di fibrillazione atriale o ritmo sinusale su un tracciato classificabile. **L'app ECG non è consigliata agli utenti a cui sono state diagnosticate altre forme di aritmia.**

È una funzionalità di automedicazione. **I dati mostrati dall'app ECG sono forniti esclusivamente a scopo informativo.** L'utente non deve interpretare autonomamente i dati o prendere provvedimenti clinici in base ai risultati del dispositivo senza prima aver consultato uno specialista. Il tracciato dell'elettrocardiogramma rappresenta un supplemento alla classificazione del ritmo cardiaco, con lo scopo di distinguere una presenza di fibrillazione atriale dal normale ritmo sinusale e **non è destinato a sostituire** metodi tradizionali di diagnosi e trattamento.

L'app ECG non è pensata per l'uso da parte di soggetti di età inferiore a 22 anni.

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.



AIIC 2023

FORTEZZA DA BASSO

Firenze 10-13 maggio 2023

Convegno Nazionale
Associazione Italiana Ingegneri Clinici

Innovazione e accessibilità:

il governo delle tecnologie sanitarie come sfida sociale

GDPR vs sicurezza

Considerando 83

Per **mantenere la sicurezza** e prevenire trattamenti in violazione al presente regolamento, il titolare del trattamento o il responsabile del trattamento dovrebbe **valutare i rischi inerenti al trattamento e attuare misure per limitare tali rischi**, quali la cifratura. Tali misure dovrebbero assicurare un adeguato livello di sicurezza, inclusa la riservatezza, tenuto conto dello stato dell'arte e dei costi di attuazione rispetto ai rischi che presentano i trattamenti e alla natura dei dati personali da proteggere. Nella valutazione del rischio per la sicurezza dei dati è opportuno tenere in considerazione i **rischi presentati** dal trattamento dei dati personali, **come la distruzione accidentale o illegale, la perdita, la modifica, la rivelazione o l'accesso non autorizzati a dati personali trasmessi, conservati o comunque elaborati, che potrebbero cagionare in particolare un danno fisico, materiale o immateriale.**

Articolo 32 Sicurezza del trattamento

1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento **mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio**, che comprendono, tra le altre, se del caso:

- a) la pseudonimizzazione e la cifratura dei dati personali;
- b) la capacità di assicurare su base permanente la **riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento**;
- c) **la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico**;

Articolo 32

Sicurezza del trattamento

d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

2. Nel valutare **l'adeguato livello di sicurezza**, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.
3. L'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo.
4. Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

AIIC 2023

FORTEZZA DA BASSO

Firenze 10-13 maggio 2023

Convegno Nazionale
Associazione Italiana Ingegneri Clinici

Innovazione e accessibilità:

il governo delle tecnologie sanitarie come sfida sociale

Sicurezza MDR e IVDR

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)

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

23.4 - Informazioni contenute nelle istruzioni per l'uso

a ter) per i dispositivi che contengono sistemi elettronici programmabili, compreso un software, o per i software che costituiscono dispositivi a sé stanti, 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.**

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.**

REQUISITI RELATIVI ALLA PROGETTAZIONE E ALLA FABBRICAZIONE

18. Dispositivi attivi e dispositivi a essi collegati

- 18.8. I dispositivi sono progettati e fabbricati in modo tale da **proteggerli**, per quanto possibile, **da accessi non autorizzati che potrebbero impedire loro di funzionare come previsto**. **Cybersecurity?**

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.

REQUISITI RELATIVI ALLA PROGETTAZIONE E ALLA FABBRICAZIONE

18. Dispositivi attivi e dispositivi a essi collegati

- 18.8. I dispositivi sono progettati e fabbricati in modo tale da **proteggerli**, per quanto possibile, **da accessi non autorizzati che potrebbero impedire loro di funzionare come previsto**. **Cybersecurity?**

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

L'associazione francese Sniterm (imprese tecnologia medica), 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”**

AIIC 2023

FORTEZZA DA BASSO

Firenze 10-13 maggio 2023

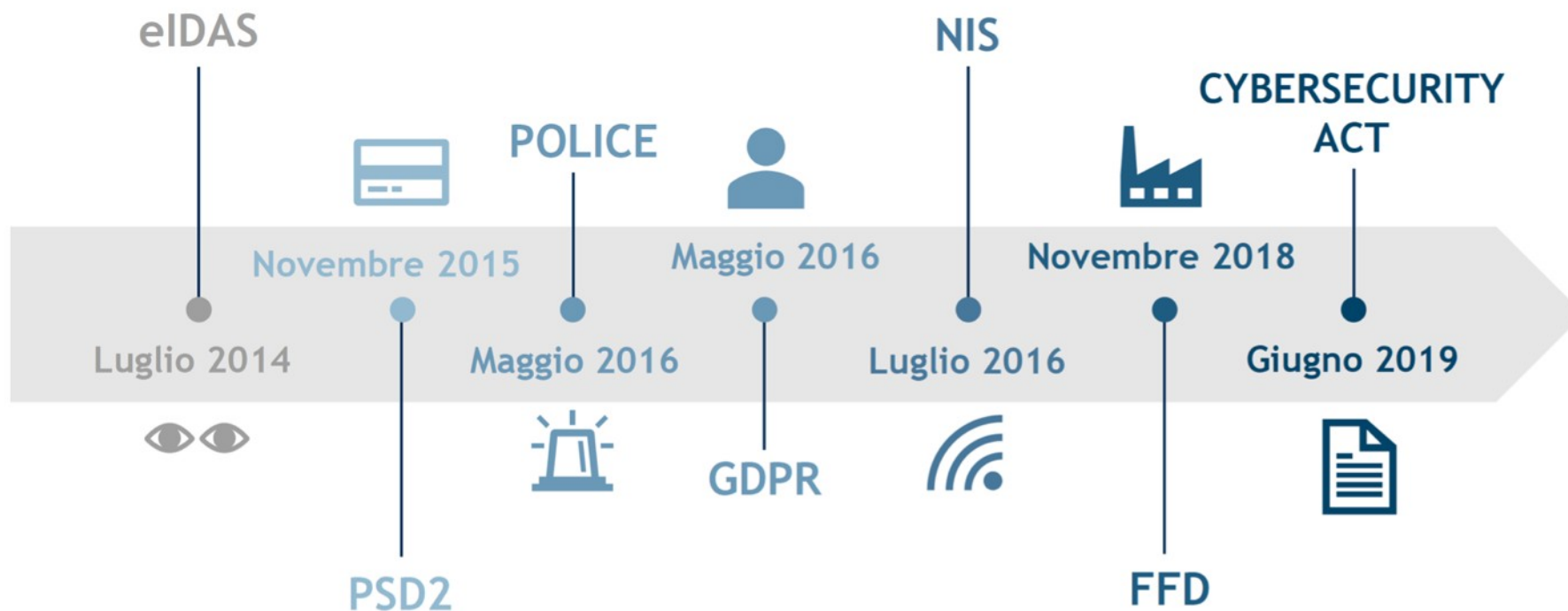
Convegno Nazionale
Associazione Italiana Ingegneri Clinici

Innovazione e accessibilità:

il governo delle tecnologie sanitarie come sfida sociale

Armonizzazione sicurezza

Information security e data protection



Information security e data protection

GDPR	POLICE	NIS	eIDAS	PSD2
Art. 32	Art. 29	Art. 16	Art. 19	Art. 95
Misure tecniche e organizzative	Misure tecniche e organizzative	Misure tecniche e organizzative	Misure tecniche e organizzative	Quadro di misure di mitigazione e meccanismi di controllo
Adeguate per garantire un livello di sicurezza adeguato al rischio	Adeguate per garantire un livello di sicurezza adeguato al rischio	Adeguate e proporzionate alla gestione dei rischi posti alla sicurezza della rete e dei sistemi informativi	Appropriate per gestire i rischi legati alla sicurezza dei servizi fiduciari	Adeguati per gestire i rischi operativi e di sicurezza
Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento	Tenuto conto dello stato dell'arte, dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento	Tenuto conto delle conoscenze più aggiornate in materia	Tenuto conto degli ultimi sviluppi tecnologici	–

Information security e data protection

GDPR

POLICE

NIS

eIDAS

PSD2

Art. 33/34	Art. 30/31	Art. 16	Art. 19	Art. 96
Violazione dei dati personali	Violazione dei dati personali	Qualsiasi incidente avente un impatto rilevante sulla fornitura di un servizio digitale	Violazioni sicurezza o perdite di integrità con impatto significativo su servizi fiduciari prestati o su dati pers.	Grave incidente operativo o relativo alla sicurezza
Notifica Autorità di controllo competente/interessati*	Notifica Autorità di controllo competente/interessati*	Notifica Autorità competente o CSIRT	Notifica organismo di vigilanza e ad altri organismi interessati//a p. fisiche o giuridiche*/ENISA*	Notifica autorità competente/utenti di servizio di pagamento*
Senza ingiustificato ritardo Entro 72 ore (ove possibile)	Senza ingiustificato ritardo Entro 72 ore (ove possibile)	Senza indebito ritardo	Senza indugio ma in ogni caso entro 24 ore dall'esserne venuti a conoscenza	
Natura violazione, categorie e numero di interessati e di registrazioni dei dati	Natura violazione, categorie e numero di interessati e di registrazioni dei dati	Numero di utenti interessati Durata dell'incidente Diffusione geografica Portata della perturbazione	-	-
Nome e contatto DPO o altro punto di contatto	Nome e contatto DPO o altro punto di contatto	Portata dell'impatto sulle attività economiche e sociali	-	-
Probabili conseguenze	Probabili conseguenze		-	-
Misure adottate o proposte per rimediare/attenuare	Misure adottate o proposte per rimediare/attenuare		-	-

Le definizioni di Cybersecurity e Cybersafety

Cybersecurity :

la capacità di una rete e dei sistemi informativi di resistere, a un determinato livello di riservatezza, a ogni azione che comprometta la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati o trasmessi o trattati e dei relativi servizi offerti o accessibili tramite tale rete o sistemi informativi.

Direttiva UE 2016/1148, art. 4

Cybersafety:

sicurezza informatica sotto il profilo della progettazione, della costruzione e della manutenzione di un sistema affinché il sistema stesso non pregiudichi l'incolumità o la salute delle persone

Cybersecurity MD:

is the process of preventing unauthorized access, modification, misuse or denial of use, or the unauthorized use of information that is stored, accessed, or transferred from a medical device to an external recipient.

AIIC 2023

FORTEZZA DA BASSO

Firenze 10-13 maggio 2023

Convegno Nazionale
Associazione Italiana Ingegneri Clinici

Innovazione e accessibilità:

il governo delle tecnologie sanitarie come sfida sociale

CYBERSECURITY

Cybersecurity, di cosa parliamo?

NIST IR 7298 Revision 2, *Glossary of Key Information Security Terms*

cybersecurity |,sībərsi'kyooritē| :

The ability to protect or defend the use of cyberspace from cyber attacks.

Or

The **process** of protecting information by **preventing, detecting, and responding** to **attacks**.

Cyberspace:

A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

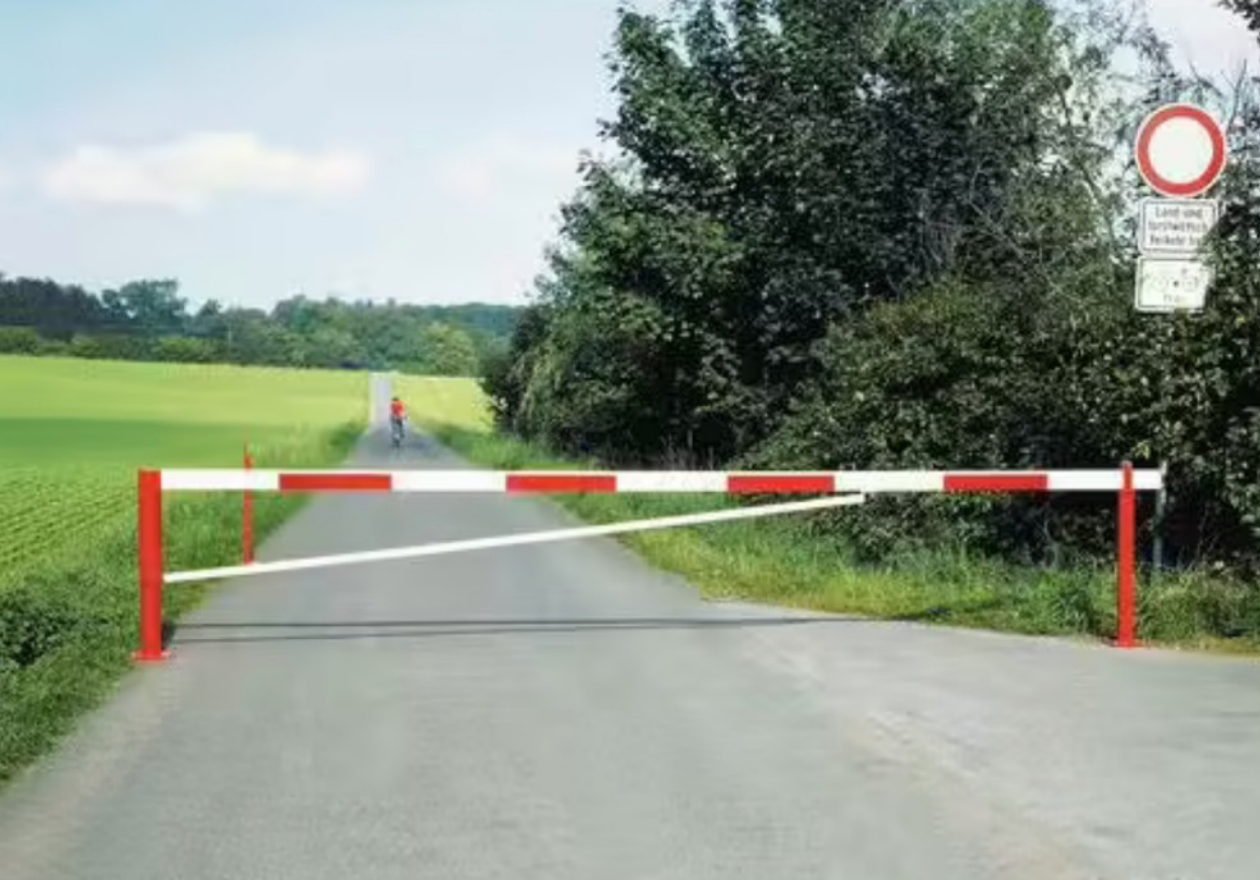
Cyber Attack:

An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information

Ma i Clinici sono un ostacolo alla Cybersecurity?

- Fallo funzionare e «non scocciarmi» con le password
- Ma non posso vedere le immagini sul mio tablet?
- Non si può collegare in rete?
- Posso avere internet sulla workstation di refertazione
- Preferisco usare il mio smartphone
- Perché in sala operatoria la rete non «prende»
- Mandami pure il referto sul mio smartphone/tablet
- Non ho tempo da perdere io faccio il medico





Le Regole non rispettate

Cambio di prospettiva:

*sviluppare partnership
sulla sicurezza
informatica con i clinici*



Consapevolezza

- Viviamo in un ambiente ostile per la protezione di sistemi e dati
- Difficile raggiungere la sicurezza reale di dati, informazioni e sistemi



Le nostre città: da
fortezze a luoghi
iper-connessi





Ma quali sono i rischi?

Il rischio e la sua percezione

I rischi associati ad un **progetto** possono essere grossolanamente sottostimati se alcuni pericoli non sono percepiti o non conosciuti



*Tversky and
Kahneman,
Judgment
Under
Uncertainty,
1974 (il paper ha
[42816](#) citazioni)*




Distrazione

- Mancata prescrizione di un farmaco;
- mancata visione di un allarme.



Risk Management and Healthcare Policy

Dovepress
open access to scientific and medical research

 Open Access Full Text Article

METHODOLOGY

Distraction: an assessment of smartphone usage in health care work settings

This article was published in the following Dove Press journal:
Risk Management and Healthcare Policy
28 August 2012

[Number of times this article has been viewed](#)

Preetinder S Gill¹
Ashwini Kamath²
Tejkaran S Gill³

¹College of Technology, Eastern Michigan University, Ypsilanti, MI, USA;

²School of Information, University

Abstract: Smartphone use in health care work settings presents both opportunities and challenges. The benefits could be severely undermined if abuse and overuse are not kept in check. This practice-focused research paper examines the current panorama of health software applications. Findings from existing research are consolidated to elucidate the level and effects of distraction in health care work settings due to smartphone use. A conceptual framework for crafting guidelines to regulate the use of smartphones in health care work settings is then

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

Perdita di dati
importanti



Clinici: da scettici a partner della sicurezza cyber

**Not “If,”
But “When”**



- Coinvolgimento già dalla fase di acquisto e avvio
- formazione
- Superamento del concetto di sicurezza IT come barriera
- Importanza dei concetti di Usability e User Experience
- Effetti della distrazione
- Effetti sulla sicurezza del paziente
- Simulazioni
<https://www.youtube.com/watch?v=OpyYLJOLwpA>
- Zero trust
- Attacco cyber: la domanda non è se, ma quando....

La formazione

- Formazione personalizzata per diverse specialità
- Nuove figure professionali come i CISO e CMIO
- Costituire un TIM
 - CMIO
 - CISO
 - Clinical engineering leadership,
 - emergency manager,
 - residents, fellows, nurses, etc,
“medical device cybersecurity committee”

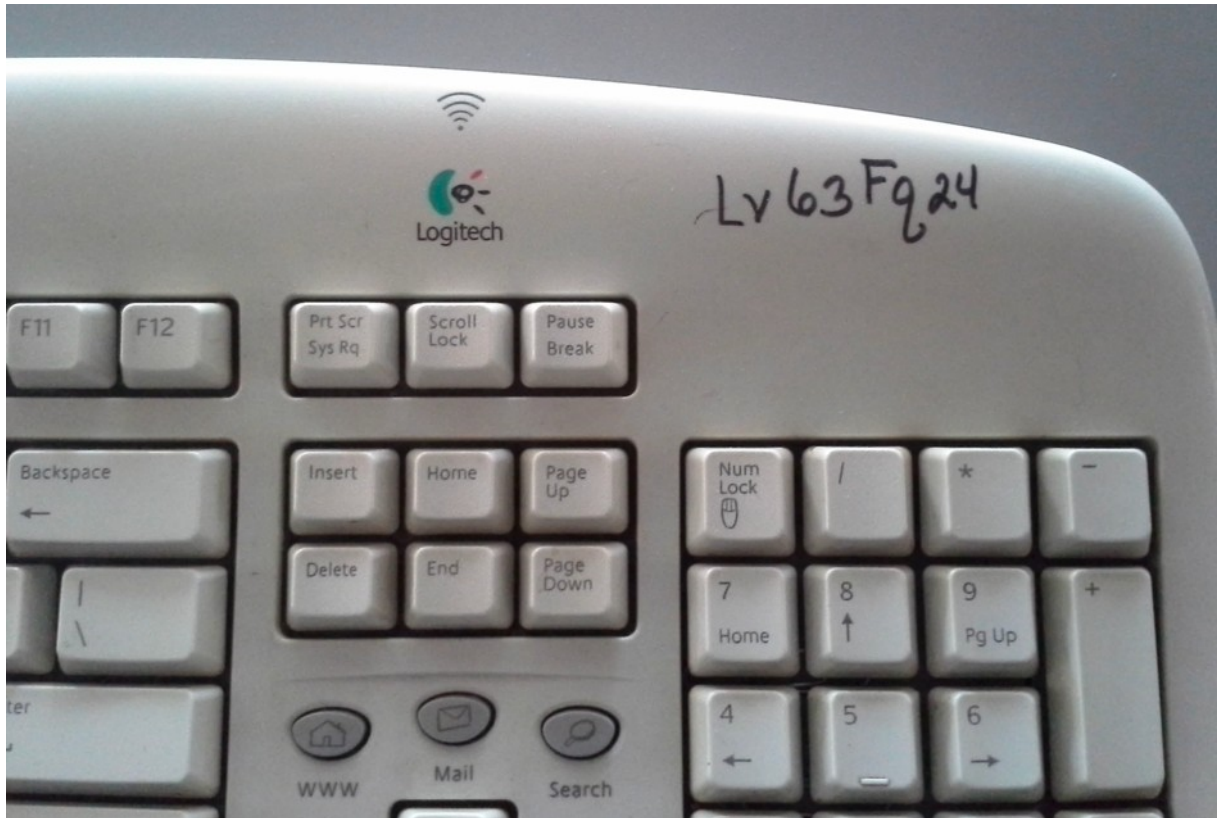


Dati e comportamenti

- Aspetto importante della sicurezza informatica (riferimenti anche nel regolamento MD)
- Comportamenti sbagliati invalidano le misure più sofisticate di protezione
- Controllo dei comportamenti con policy, formazione, certificazioni, norme tecniche, qualità



Le PassWord





La frase più pericolosa in assoluto è:

«Abbiamo sempre fatto così!»

Grace Murray Hopper



Sicurezza Informatica

- Riservatezza (Confidenzialità)

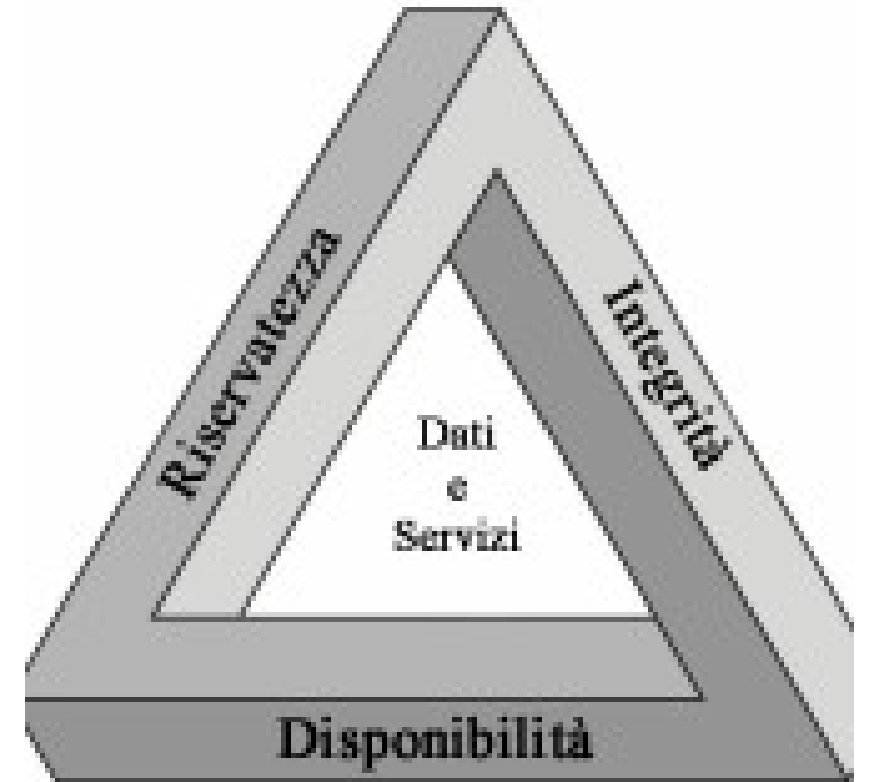
la protezione delle informazioni mediante l'accesso consentito soltanto agli autorizzati, la protezione delle trasmissioni, il controllo degli accessi, ...


- Integrità

la salvaguardia della correttezza dei dati, la difesa dalle manomissioni e da modifiche non autorizzate, il monitoraggio automatico degli accessi, ...

- Disponibilità

la garanzia per gli utenti di poter disporre dei dati, delle informazioni e dei servizi, evitando la loro perdita o riduzione





“ There’s a storm on the horizon, and it may already be here. Healthcare security is no longer [just] a compliance issue. It’s not only about protecting ePHI. It’s a patient safety issue.”

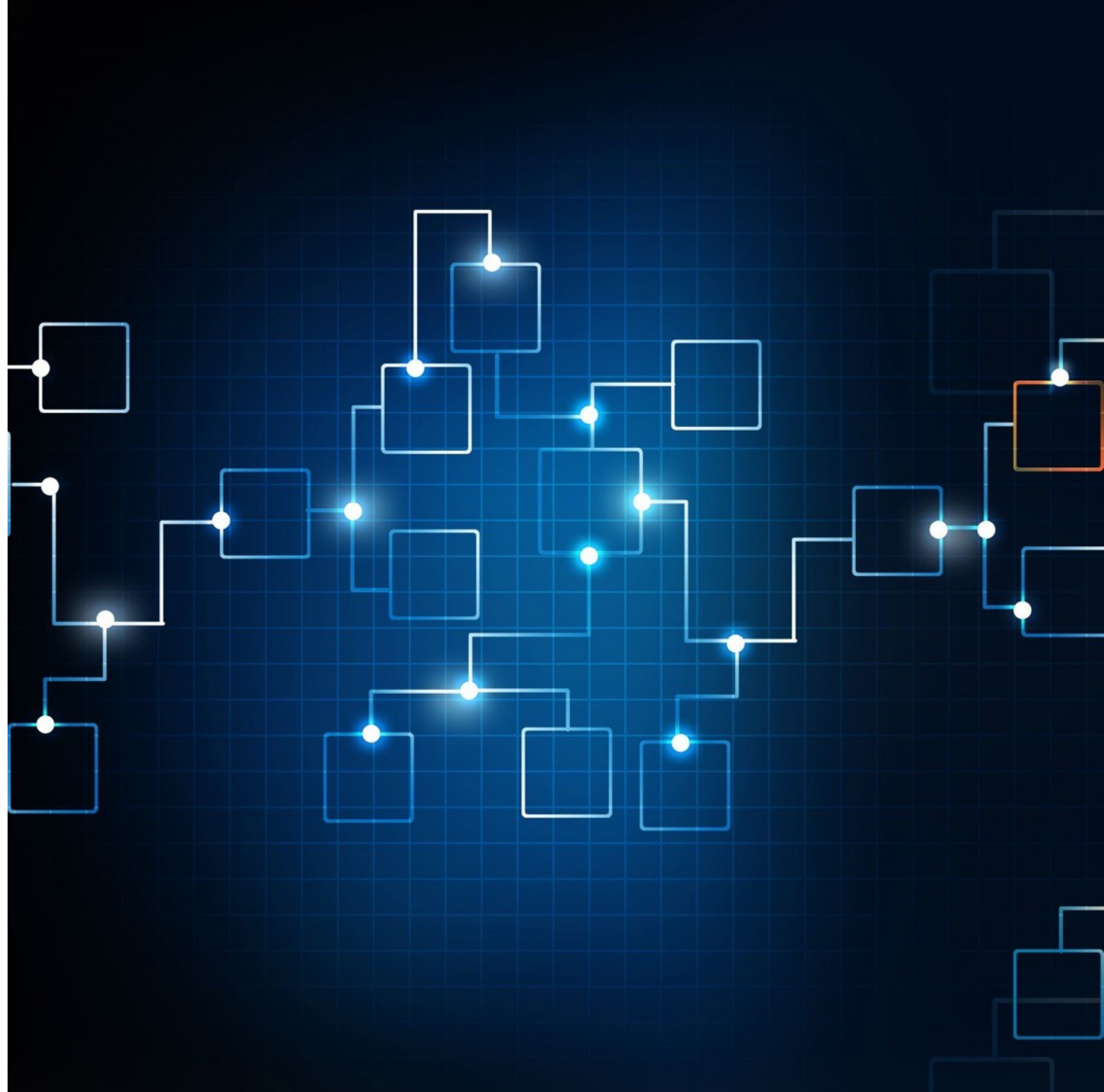
**Jeffrey Tully, Security Researcher, UC Davis
HIMSS Security Forum**

Introducing new technology

OO plus NT equals COO

which stands for

(old organization plus new technology) equals (costly old organization)



Procurement actors

- HDO Healthcare Technology Management
 - Clinical Features
 - Security
- MDM Medical Device Manufactures
 - Process



Procurement key Points

1) INFORMATION

- MDM processes vs secure development, vulnerability management, coordinated vulnerability disclosures, incident response
- Security update
- Share vulnerabilities

2) MDM Strong Organization on cybersecurity support

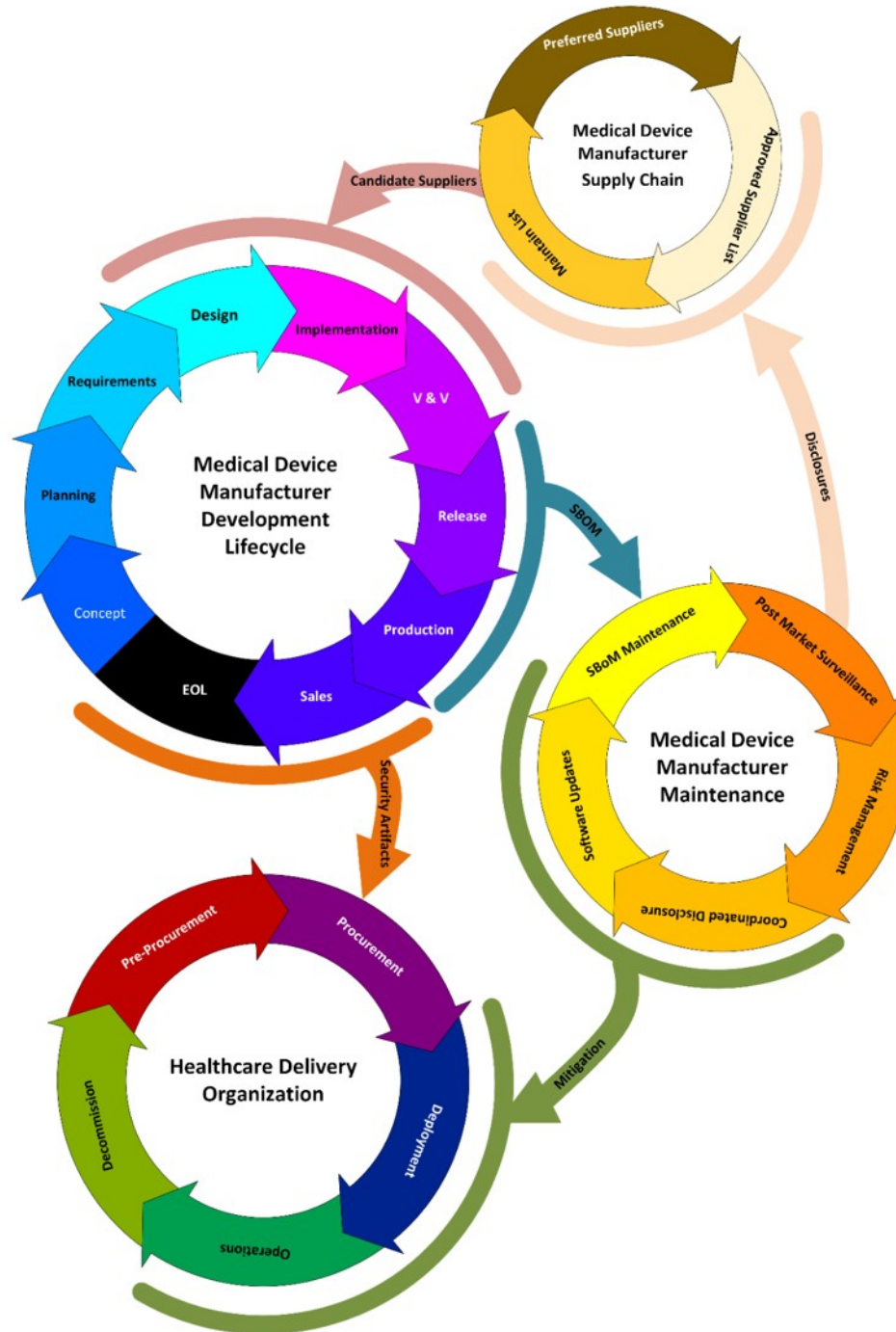
3) MDS2 FORM (2019 version)

4) DEVICE «SECURE BY DESIGN»

Manufacturer Disclosure Statement for Medical Device Security (MDS2)

Manufacturer Disclosure Statement for Medical Device Security – MDS ²										
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?							_____	_____	_____	_____

Areas and Phases of Lifecycle Management

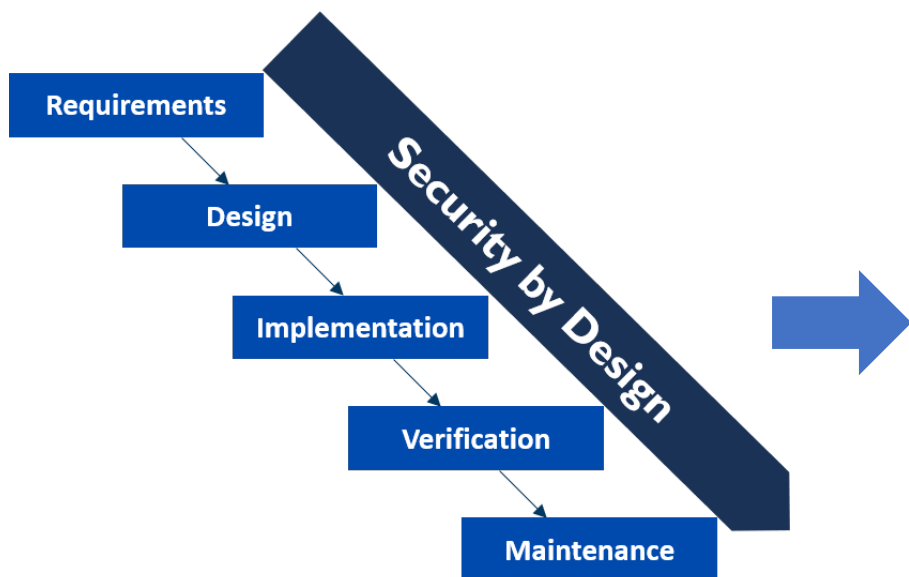


Come l'industria dovrà affrontare i rischi informatici

Punti chiave:

1. Inserire la sicurezza informatica direttamente nella fase **progettuale e di sviluppo del prodotto**.
2. Effettuare una revisione dei **rischi**, delle **minacce** e delle **vulnerabilità** del dispositivo e documentare le scoperte e proattivamente identificare nuove potenziali minacce.
3. Assicurarsi che il software del dispositivo sia **accuratamente testato**.
4. Esaminare il **ciclo di vita** dei dati in modo che sia trasparente quali dati sono stati creati e dove e come questi saranno elaborati.
5. Creare e mantenere un registro dei rischi e dei reclami e non conformità.
6. Revisione ed aggiornamento del prodotto e della documentazione (audit check) sulla base delle modifiche alle leggi internazionali.
7. Creare e mantenere un **registro dei rischi** e dei **reclami** e **non conformità**.
8. Formazione tecnica del **personale qualificato**.
9. Includere la **sicurezza del ciclo di vita del prodotto prevista in schemi di valutazione dei rischi e di controllo**, suscettibile di essere articolata in futuro in capitolati di gara di appalti sanitari.

Cybersecurity: la strategia regolatoria



Punto di partenza: considerare gli aspetti di cybersecurity fin dalle prime fasi di sviluppo del DM (vedi All. I – GSPR + norme tecniche ISO 14971, ISO 27001, IEC 80001-1, IEC 62304, IEC 82304-1).



Uso sicuro del DM, fornendo ai pazienti e/o agli utilizzatori tutte le informazioni necessarie, comprese le buone pratiche di “**cyber igiene**”.



Collaborazione con clienti, operatori sanitari, pazienti, ricercatori sulla sicurezza e altri, verso l'obiettivo della «**sicurezza attraverso la partnership**». Le aziende possono emettere regolarmente divulgazioni di sicurezza coordinate volontarie, al fine di condividere informazioni con i clienti sulle potenziali vulnerabilità che identificano o di cui vengono a conoscenza e su come i clienti possono proteggere se stessi e i loro pazienti.

Dismissione Dispositivo Medico

Gestione dismissione



IT vs IC

- Gli ingegneri Clinici capiscono meglio come funzionano i MD e cosa succede quando non funzionano o non sono disponibili

Sfide organizzative 1/2

- La Crescita esponenziale della complessità delle tecnologie e la loro necessità di connettività ha prodotto “sistemi di sistemi” che richiedono organizzazioni (di 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



Sfide organizzative 2/2

- Le conoscenze, le abilità e le capacità necessarie per supportare i professionisti sanitari nel gestire le nuove tecnologie sanitarie non sono sempre adeguate all'evoluzione 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.



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. Può 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



Perché i dispositivi medici sono così complessi da proteggere

I dispositivi medici non condividono lo stesso ciclo di vita dei dispositivi IT:

I computer vengono sostituiti ogni 3-5 anni e perdono completamente il loro valore in 7 anni

I dispositivi medici presentano cicli di vita che in alcuni casi vanno ben oltre i 10 anni

Le organizzazioni sanitari tendono a rinviare gli investimenti di sostituzione

La sicurezza dei dispositivi medici è più complessa

Questa lunga durata comporta che la maggior parte della vita di un DM possa essere legata ad sistema operativo legacy non supportato

I sistemi operativi legacy rendono difficile la protezione di questi dispositivi, richiedendo una micro segmentazione di livello 2

Health System Roles & Responsibilities

Role	Actions for the Role
CISO/ Information Security	Accountable for the organization's security
Compliance/ Privacy	Ensures regulatory & privacy requirements are met
Supply Chain/ Vendor/ Supplier	Provides products and services to the organization
Information Technology	Provides availability of technology and services
Legal	Ensures compliance of applicable laws
Healthcare Technology Management/ CE/ Biomed	Ensures safety and reliability of clinical technologies
Corporate Communications/ Public Relations	Internal/ external messaging from the organization
Emergency Management	Manages organization's impacting incidents
Clinical Risk Management	Accountable for the organization's patient and caregiver safety
Nursing/ Physician Leadership	Manages nursing and physician teams and workflows for patient care
Note Taker	Records all responses for the team
Spokesperson	Shares responses from the team

Approccio alla CYBERSECURITY per IC

- Approccio diverso dal modo tradizionale ICT
- Non basta una patch
- Importanza dell'analisi del parco macchine
- Gestione degli assett medicali
- Conseguenze sulla sicurezza di non separare l'OT dall'IT by design
- aumento dell'uso di dispositivi wireless, Internet e connessi alla rete, supporti portatili
- I dispositivi sicuri ed efficaci sono essenziali per un'efficace assistenza ai pazienti e nell'assistenza sanitaria

Approccio alla CYBERSECURITY per IC

Software as a Medical Device (SaMD) e Software in a Medical Device (SiMD), vs definizione di software critico

- **Allinea i tuoi team IT/Sicurezza e Ingegneria Clinica**
- Non trattare i dispositivi medici come normali endpoint IT o dispositivi Internet of Things (IoT). Assicurarsi che tutte le patch, gli aggiornamenti e/o le soluzioni di sicurezza degli endpoint siano stati convalidati dall'OEM prima di essere installati. Richiedere istruzioni scritte, documentazione e manuali aggiornati, se necessario.
- collaborazione tra i team di ingegneria clinica e IT/sicurezza

Care delivery
and patient
safety

IT Security
measures

device
availability

Usability,
functionality

Patching,
vulnerability test

hardening

Security benefits



Gestione e manutenzione



- La gestione e manutenzione dei dispositivi medici differisce dalle analoghe attività dai sistemi IT.
- La cybersecurity per i sistemi IT è più matura e la relativa omogeneità dei sistemi IT consente la gestione delle patch, la scansione delle vulnerabilità, il software antivirus, la gestione delle risorse.
- Le tradizionali attività della sicurezza informatica, come la scansione delle vulnerabilità e la gestione delle patch, sono difficili da implementare per i MD. **Spesso gli assetti medicali non sono progettati per supportare questi scan. Non si possono installare agenti**
- Per i dispositivi medici IT è difficile avere un accurato inventario dei DM sw. I dispositivi "legacy" più vecchi e distribuiti rappresentano una sfida per la cybersecurity
- La cybersecurity è un processo dinamico e mantenere sicuri i dispositivi è un'attività complessa
- Mondo DM fatto di tanti produttori e modelli difficile da seguire

Gestione e manutenzione



- I produttori devono condividere informazioni sul software che usano nei loro prodotti (ad es., Quale versione di un sistema operativo incorporato è in uso). La versione 2013 di MDS2 aiuta ma non è sempre disponibile o completa.
- Difficile tenere traccia dei sistemi operativi, delle versioni software e di altre informazioni rilevanti per la sicurezza IT.
- I produttori devono condividere informazioni sullo stato della gestione delle patch per i loro dispositivi e, quando vengono testate le patch, completare il test e la raccomandazione finale in un ragionevole periodo di tempo.

Gestione e manutenzione 1/2



- Sottoporre a scansioni di vulnerabilità anche i dispositivi medici connessi in rete al fine di identificare le vulnerabilità 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 periferiche 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

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.

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 CS ² , Avance, Amingo, Avance CS ²	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.

Le Misure Minime di sicurezza



Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri
Area Sistemi, tecnologie e sicurezza informatica

MISURE MINIME DI SICUREZZA ICT PER LE PUBBLICHE AMMINISTRAZIONI

(Direttiva del Presidente del Consiglio dei Ministri 1 agosto 2015)

26 APRILE 2016

Agenzia per l'Italia Digitale 26 aprile 2016
Misure minime di sicurezza ICT per le Pubbliche Amministrazioni

INDICE

1 GENERALITÀ	3
1.1 SCOPO	3
1.2 STORIA DELLE MODIFICHE	3
1.3 RIFERIMENTI	3
1.4 ACRONIMI	3
2 PREMessa	4
3 LA MINACCIA CIBERNETICA PER LA PA	6
ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI	7
ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI	9
ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER	10
ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ	12
ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE	14
ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE	17
ABSC 10 (CSC 10): COPIE DI SICUREZZA	19
ABSC 13 (CSC 13): PROTEZIONE DEI DATI	20

Già anticipate via Web
sin da settembre 2016

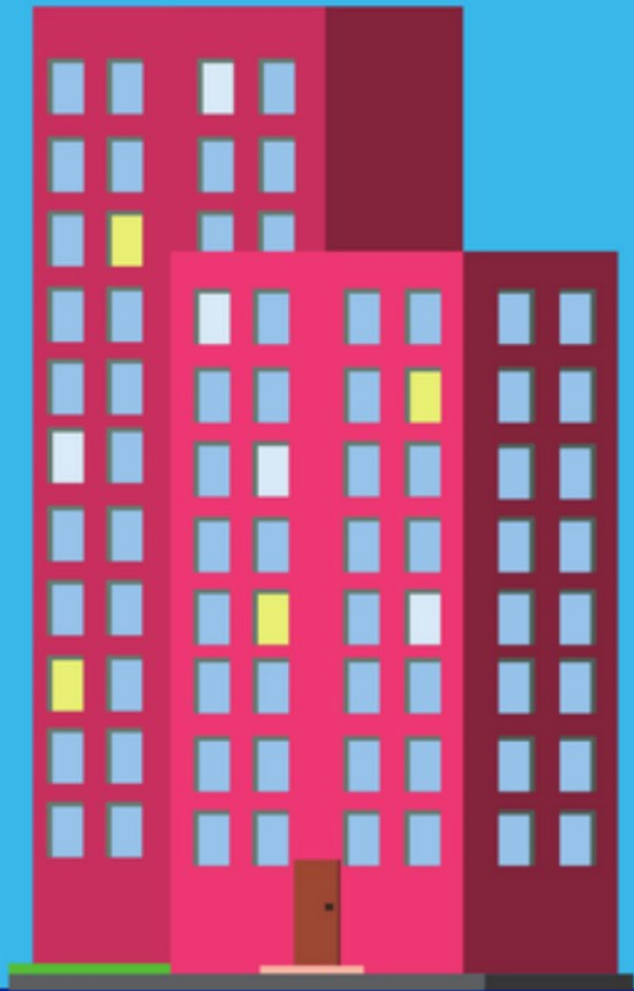
Emesse con circolare
18 aprile 2017, n. 2/2017

Gazzetta Ufficiale (SG)
n.103 del 5/5/2017

Adozione obbligatoria
entro il 31/12/2017

Dovere d'ufficio del Dirigente
responsabile IT (art. 17 CAD)





PROTECTING YOUR BUILDING: CYBERSECURITY IN BUILDING AUTOMATION



CYBERSECURITY

by Michael Chipley PhD, PMP, LEED AP

The PMC Group LLC

Updated: 03-27-2017

Updated:
02-21-2020

INTRODUCTION

Industrial Control Systems (ICS) are physical equipment oriented technologies and systems that deal with the actual running of plants and equipment, include devices that ensure physical system integrity and meet technical constraints, and are event-driven and frequently real-time software applications or devices with embedded software. These types of specialized systems are pervasive throughout the infrastructure and are required to meet numerous and often conflicting safety, performance, security, reliability, and operational requirements. ICSs range from building environmental controls (HVAC, lighting), to systems such as the electrical power grid. With the increasing interconnectivity of ICS to the internet, the ICS can be an entry point into the organization's other IT systems.

Within the controls systems industry, ICS systems are often referred to as Operational Technology (OT) systems. Historically, the majority of OT systems were proprietary, analog, vendor supported, and were not internet protocol (IP) enabled. Systems key components, such as Remote Terminal Units (RTUs), Programmable Logic Controllers (PLCs), Physical Access Control Systems (PACs), Intrusion Detection Systems (IDSs), closed circuit television (CCTV), fire alarm systems, and utility meters have become digital and IP enabled. OT systems use Human Machine Interfaces (HMIs) to monitor the processes, versus Graphical User Interfaces for IT systems. Most current ICS systems and subsystems are now a combination of Operational Technologies (OT) and Information Technologies (IT).

WITHIN THIS PAGE

- [Introduction](#)
- [Description](#)
- [Additional Resources](#)

Industrial Control Systems (ICS) & Operational Technology (OT)

- Supervisory Control and Data Acquisition (Energy, Water, Wastewater, Pipeline, Airfield Lighting, Locks, and Dams, etc.)
- Distributed Control Systems (Process and Manufacturing, etc.)
- Building Control Systems/Building Automation Systems
- Utility Management Control Systems
- Electronic Security Systems
- Fire, Life Safety, Emergency Management Systems
- Exterior Lighting and Messaging Systems
- Intelligent Transportation Systems

Table 1—IT vs. OT Systems Comparison

	INFORMATION TECHNOLOGY	OPERATIONAL TECHNOLOGY
Purpose	Process transactions, provide information	Control or monitor physical processes and equipment
Architecture	Enterprise wide infrastructure and applications (generic)	Event-driven, real-time, embedded hardware and software (custom)
Interfaces	GUI, Web browser, terminal and keyboard	Electromechanical, sensors, actuators, coded displays, hand-held devices
Ownership	CIO and IT	Engineers, technicians, operators and managers
Connectivity	Corporate network, IP-based	Control networks, hard wired twisted pair and IP-based
Role	Supports people	Controls machines

Power over Ethernet (PoE)

Smart Building

- convergence of the IT and OT into a new hybrid where the CIO provides the switches, routers and firewalls as Government Furnished Equipment (GFE), and all the building monitoring and control systems plug into the CIO fiber backbone in the distribution closet, as shown in Figure 7.

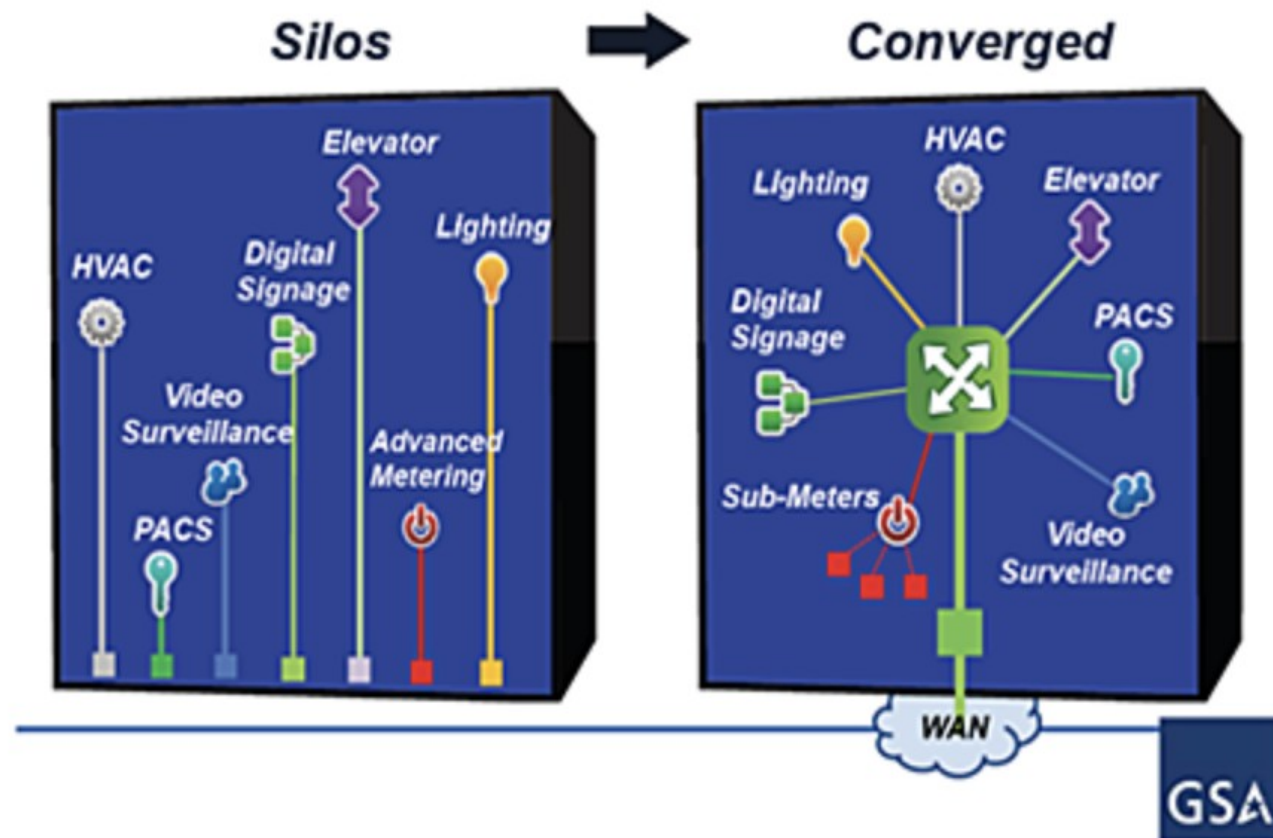


Figure 7: Converged Building M&C Connected in the Distribution Closet

NIST Special Publication 800-82

Revision 2

Guide to Industrial Control Systems (ICS) Security

**Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS),
and Other Control System Configurations such as Programmable Logic Controllers (PLC)**

Keith Stouffer
Victoria Pillitteri
Suzanne Lightman
Marshall Abrams
Adam Hahn

- <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf>

da Ricordare

Art. 640-ter. Frode informatica.

Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 51 a euro 1.032.

La pena è della reclusione da uno a cinque anni e della multa da euro 309 a euro 1.549 se ricorre una delle circostanze previste dal numero 1) del secondo comma dell'articolo 640, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema.

La pena è della reclusione da due a sei anni e della multa da euro 600 a euro 3.000 se il fatto è commesso con furto o indebito utilizzo dell'identità digitale in danno di uno o più soggetti. (1)

Il delitto è punibile a querela della persona offesa salvo che ricorra taluna delle circostanze di cui al secondo e terzo comma o un'altra circostanza aggravante. (2)

(1) Comma inserito dall'art. 9, comma 1, lett. a), D.L. 14 agosto 2013, n. 933, convertito, con modificazioni, dalla L. 15 ottobre 2013, n. 119.

(2) Comma così modificato dall'art. 9, comma 1, lett. b), D.L. 14 agosto 2013, n. 933, convertito, con modificazioni, dalla L. 15 ottobre 2013, n. 119.

HIMSS 2022 HEALTHCARE CYBERSECURITY SURVEY

Type of Third-Party Services Used	Percent
Penetration testing	66.67%
Endpoint security	56.60%
Security audits	54.09%
Threat intelligence	50.94%
Risk assessments and risk management	44.65%
Cloud security	42.77%
Identity and access management	39.62%
Digital forensics (post-incident)	35.85%
Infrastructure security	33.96%
Incident response	32.70%
Application security	30.19%
Compliance	29.56%
Security operations	28.30%
Threat hunting	26.42%



HIMSS 2022 HEALTHCARE CYBERSECURITY SURVEY

Table 7: Barriers to Achieving More Robust Cybersecurity

Barriers	Percent
Lack of cybersecurity staff (inadequate numbers)	61.01%
Lack of budget	50.31%
Lack of data inventory (knowing what kind of data we have & where)	44.65%
Lack of data classification (e.g., PHI, PII, IP, etc.)	38.36%
Lack of certain specialized skills for cybersecurity staff	37.74%
Lack of cooperation by people within the organization	31.45%
Policies and procedures do not reflect current practices	30.82%
Lack of awareness about policies and procedures	29.56%
Lack of executive buy-in	22.64%
Lack of interdisciplinary teams	21.38%
Lack of leadership	15.09%
Policies and procedures are difficult to understand	13.84%
Other	2.52%
None – no barriers are present	10.69%

Table 8: Type of Authentication Implemented

Authentication Type Implemented	Percent
Multi-factor authentication – Password + Authenticator app	79.87%
Multi-factor authentication - Password + SMS code	58.49%
Basic authentication - usernames and passwords	57.23%
Multi-factor authentication - Password + Phone Call (for receiving code)	35.22%
Multi-factor authentication – Password + Hardware token	34.59%
Multi-factor authentication – Password + Biometric factor	18.87%
Biometric authentication (single factor)	16.98%
Multi-factor authentication – Passwordless	9.43%
Other	4.40%

HIMSS 2022 HEALTHCARE CYBERSECURITY SURVEY

IMPROVEMENTS

Workforce:

- More frequent, practical cybersecurity training for everyone
- Broader awareness training for everyone
- Hiring and retaining qualified cybersecurity professionals

Technical:

- Passwordless multi-factor authentication
- Robust incident response teams
- Digital forensics (post-incident)
- Third party vendors – leveraging third party expertise to reduce organizational risk
- Information sharing about threats and mitigations with peers
- Insider threat detection

Conclusion

The findings of the **2022 HIMSS Healthcare Cybersecurity Survey** suggest that healthcare organizations have made significant progress in improving their healthcare cybersecurity programs, but challenges still exist. These barriers to progress include security budgets, insufficient staff and training, and the growing volume of cyber-attacks and compromises. But perhaps the biggest vulnerability is the human factor. Healthcare organizations should do more to support healthcare cybersecurity professionals and their cybersecurity programs.

THE FUTURE OF HEALTHCARE CYBERSECURITY

• GOVERNANCE

- The success or failure of any organization is based upon how well it is **governed**.
- Are **patient safety** and **cybersecurity** top business priorities at your organization?
- Is leadership at your organization supporting the organization's cybersecurity program?
- Do the policies and procedures at your organization reflect **actual practices**?
- Are there numerous **exceptions** to the policies and procedures?
- Do **business leaders** make decisions on what information needs to be protected and why?
 - Cybersecurity professionals excel at tactics and technical know-how.
- Is the human resources department tightly integrated with the information technology department?
 - Do you know who is coming and going from your organization? (Are accounts timely provisioned and deprovisioned?)
- Is your **board of directors** informed about cybersecurity incidents and improvements/changes to the cybersecurity program?
- Does your organization have a formal **insider threat** program (e.g., policies, procedures, training, etc.)?

THE FUTURE OF HEALTHCARE CYBERSECURITY

- **Identity and Access Management**

- **Timely provisioning and deprovisioning** of accounts is **essential**

- Dormant accounts can be a goldmine for hackers (no one is looking)
 - Large fluctuation of personnel that are within healthcare organizations (e.g., visiting researchers, interns, others)

- **Appropriate access** (principle of least privilege) based upon **role**

- Roles can change often within healthcare organizations
 - Accordingly, there must be a robust system for informing IT when there is a change in a person's role that may require different permissions

- **PRACTICAL TIP:** Implementing multi-factor authentication everywhere is highly recommended; passwordless multi-factor authentication is the future (e.g., hardware tokens or app-based tokens; use of FIDO standard, etc.)

- **Incident detection & response (enabled by artificial intelligence)**

- Automated threat feeds, log analysis, and other labor-intensive, repetitive tasks can be outsourced to AI solutions
 - **However**, AI does not (yet) rival human ingenuity. Thus, an attacker can be **creative** and think of novel and sophisticated ways to infiltrate systems and networks. This is why even the best AI system might not anticipate a threat actor's next move.
 - We still need a human to have oversight over this – a robust incident response team

THE FUTURE OF HEALTHCARE CYBERSECURITY

• Training

- **Cyber ranges** are excellent resources to help better understand **incident response**
- **Tabletop exercises** (e.g., simulated scenarios) are great ways to understand how your team might handle a suspected security incident
- **Simulated phishing exercises** can provide visibility into how well your anti-phishing program is working
 - **Keeping metrics on phishing attempts and repeat offenders is a good idea**
- **Security awareness training** should occur at least quarterly, if not more frequently (e.g., newsletters, exercises, etc.)
 - Be sure to include the informatics team and clinical team

• Information sharing

- Internal information sharing: Who does one report to? What is the chain of command? Do people know the policies and procedures? Do policies and procedures need to change based upon staff input?
 - Strategic Allies: Facilities team, human resources, legal department, chief medical information officer, chief nursing information officer, chief information security officer, chief privacy officer, patient safety officer, etc.
 - **Cross-disciplinary teams for procurement, incident response, etc.**
- External information sharing: Leverage peer-to-peer information sharing and **cross-sector** information sharing with other critical infrastructure industries (**more common ground than differences**)

THE FUTURE OF HEALTHCARE CYBERSECURITY

- Workforce development
 - Shortage of healthcare cybersecurity professionals
 - Recruit from within – e.g., analysts, informaticsts, and others
 - Internship programs for students
 - **Practical tip:** Existing staff also needs to be regularly educated and trained on healthcare cybersecurity and so an organization's support is essential!
- Zero trust
 - **Never trust, always verify**
 - Departure from **inherent trust** (e.g., simple password authentication, etc.)]
 - Requires a strong foundation of security controls
 - Requires a robust identity and access management program

AIIC 2023

FORTEZZA DA BASSO

Firenze 10-13 maggio 2023

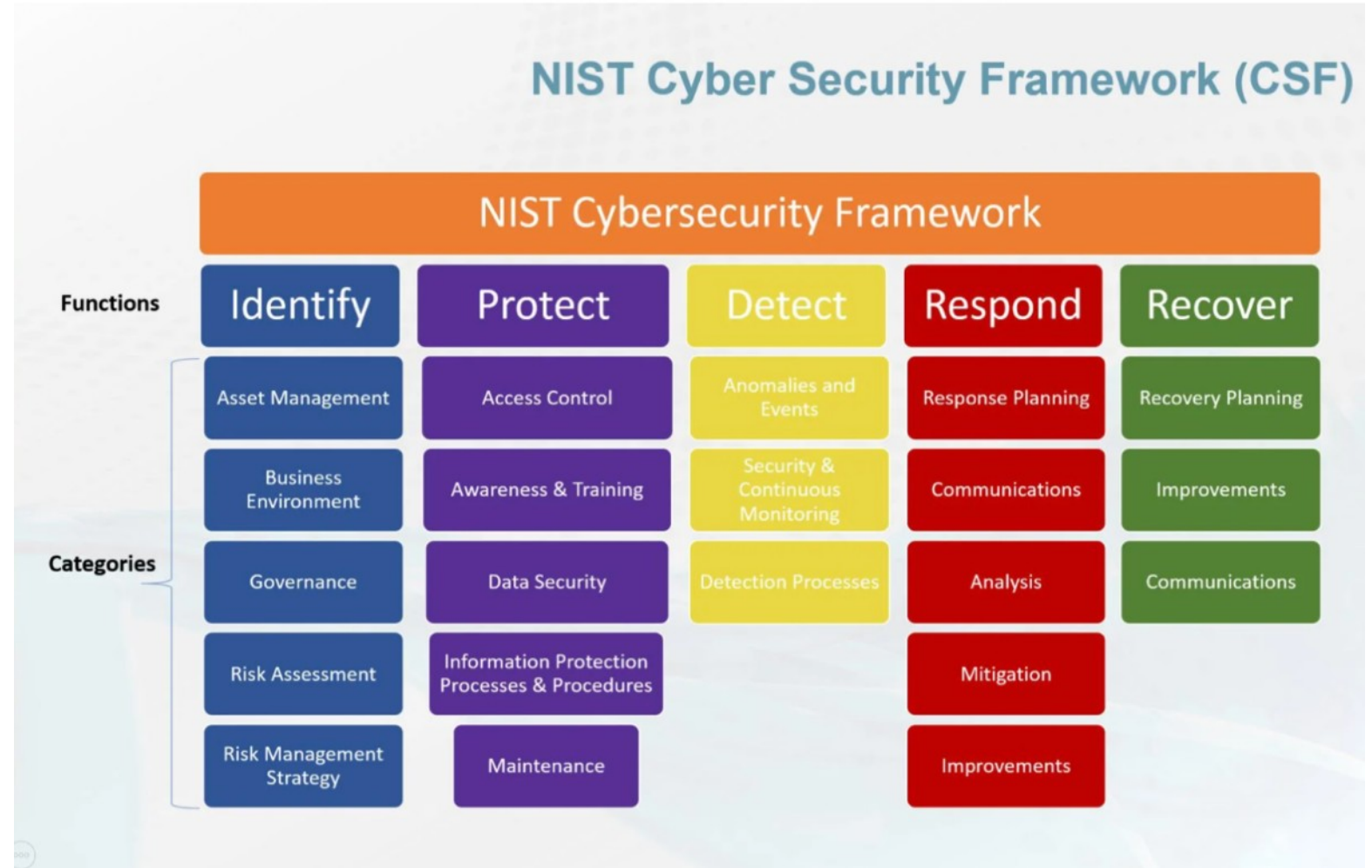
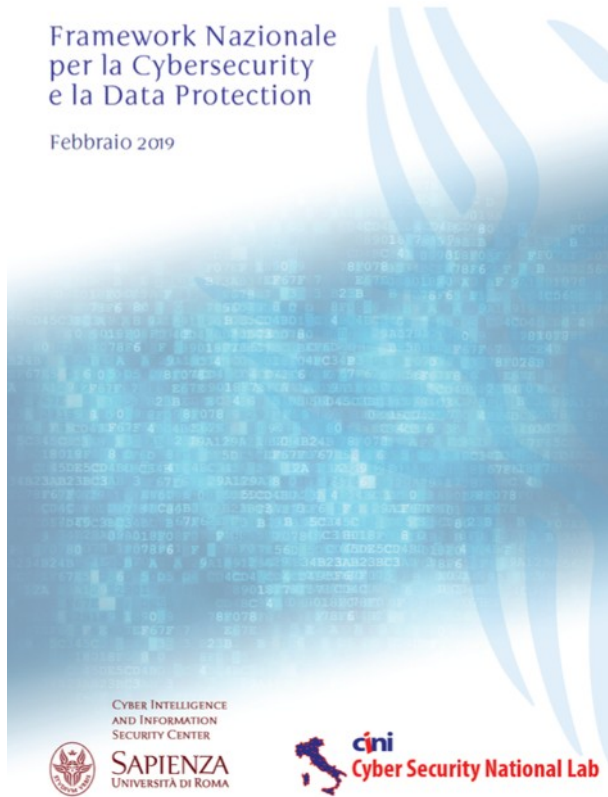
Convegno Nazionale
Associazione Italiana Ingegneri Clinici

Innovazione e accessibilità:

il governo delle tecnologie sanitarie come sfida sociale

Infine

Framework Nazionale per la Cybersecurity



SOC

Un SOC (Security Operations Center) è un centro operativo specializzato nella gestione e nel monitoraggio della sicurezza informatica di un'organizzazione. La sua principale funzione è quella di rilevare, analizzare e rispondere agli incidenti di sicurezza informatica.



Grazie per l'attenzione
Maurizio Rizzetto

- maurizio.rizzetto@asfo.sanita.fvg.it
- italianCommunity@himss.org
- maurizio.rizzetto@IHE-Italia.net