Cybersecurity e Dispositivi Medici: scenari innovativi per la sanità nell'era del cloud, dell'IoT, dei big data e del mobile computing

Michele Bava

IRCCS "Burlo Garofolo"

2 parti

Parte 1: Nuove normative tecniche e regolamenti Europei per i dispositivi medici

Parte 2: Analisi dei dati dall'utilizzo dei sistemi Medigate c/o IRCCS Burlo Garofolo

Ringraziamenti

Mead Informatica (Lisa Bassetto, Fabio Tolomelli, Mirko Gorrieri, Roberto Fantini, Giorgia Marchesi, Daniele Giacomelli)

Medigate (Offir Levy, Amit Har-Esh)

TrendMicro (Marco Iorio, Alex Galimi)

Riccardo Zangrando e Piero Pascolo e ASUFC

Parte 1

Parte 1.1: un mondo che cambia

Parte 1.2: strumenti (organizzativi), normative, norme tecniche, linee guida

Parte 1.3: modelli, tecniche e tecnologie per la cybersecurity dei DM

Parte 1.1

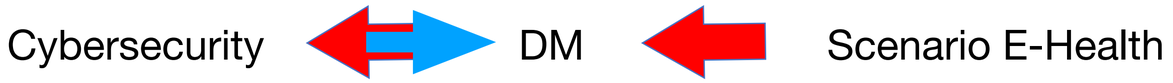
Un mondo che cambia

(La sanità in) Un mondo che cambia

E-Health e Sanità Digitale

Dispositivi medici (DM) (ambito ingegneria clinica)

Cybersecurity (ambito sistemi informativi e ICT)



Ci occupiamo di analisi e gestione del rischio dei DM e in che modo la cybersecurity e le problematiche ad essa connesse impattano su questa, su come condurla, su come eventualmente assegnare un valore del rischio ai DM e mitigarlo utilizzando della tecnologia (controllo/misura di sicurezza)

Ma cosa succede se parliamo di tutte queste cose in un contesto completamente nuovo in cui:

- cambia il nostro modo di vivere (lo stiamo sperimentando…);
- ci sono nuove sfide che la tecnologia ci pone (IoT, Cloud, m-Health, Big Data….);
- ci muoviamo in un quadro normativo in evoluzione (MDR e IVDR; norme tecniche e standard);
- cambiano gli scenari per la sicurezza, la safety e l'effectiveness;
- tecnologie, risorse, sistemi IT "escono" dall'ospedale (ospedale in uscita - sanità in uscita)
- e tutto cambia ancora… sempre (industria 5.0 -> sanità 5.0?)

(La sanità in) Un mondo che cambia

E-Health e Sanità Digitale

Dispositivi medici (DM) (ambito ingegneria clinica)

Cybersecurity (ambito sistemi informativi e ICT)

Cybersecurity ⇄ DM ⇐ Scenario E-Health

Ci occupiamo di analisi e gestione del rischio dei DM e in che modo la cybersecurity e le problematiche ad essa connesse impattano → su questa, su come condurla, su come eventualmente assegnare un valore del rischio ai DM e mitigarlo utilizzando della tecnologia (controllo/misura di sicurezza)

Ma cosa succede se parliamo di tutte queste cose in un contesto completamente nuovo in cui:

- cambia il nostro modo di lavorare e rapportarci:
  - tra noi (IT e IC)
  - con i nostri fornitori (di tecnologie IT o IC o misti)
  - con istituzioni (Regioni, Ministeri) e enti normativi (Agid)
  - in merito al procurement, ai sistemi di qualità, agli adempimenti volontari e obbligatori
  - con i nostri malati, pazienti, utenti, clienti -> ora di nuovo malati…

Scenario - E-Health

Le sfide del SSN

Il Ministro della Salute

38% è malato cronico (diabete, ipertensione, bronchite cronica e malattie connesse all'età avanzata > 65 anni)

48,7% delle persone dai 65 ai 74 anni affetto da almeno due malattie croniche

70% circa spesa sanitaria (113,1 mld finanziamento SSN)

Prevenzione?

Le sfide del SSN

Autorità Regolatorie

Invecchiamento delle popolazione

Accesso all'innovazione

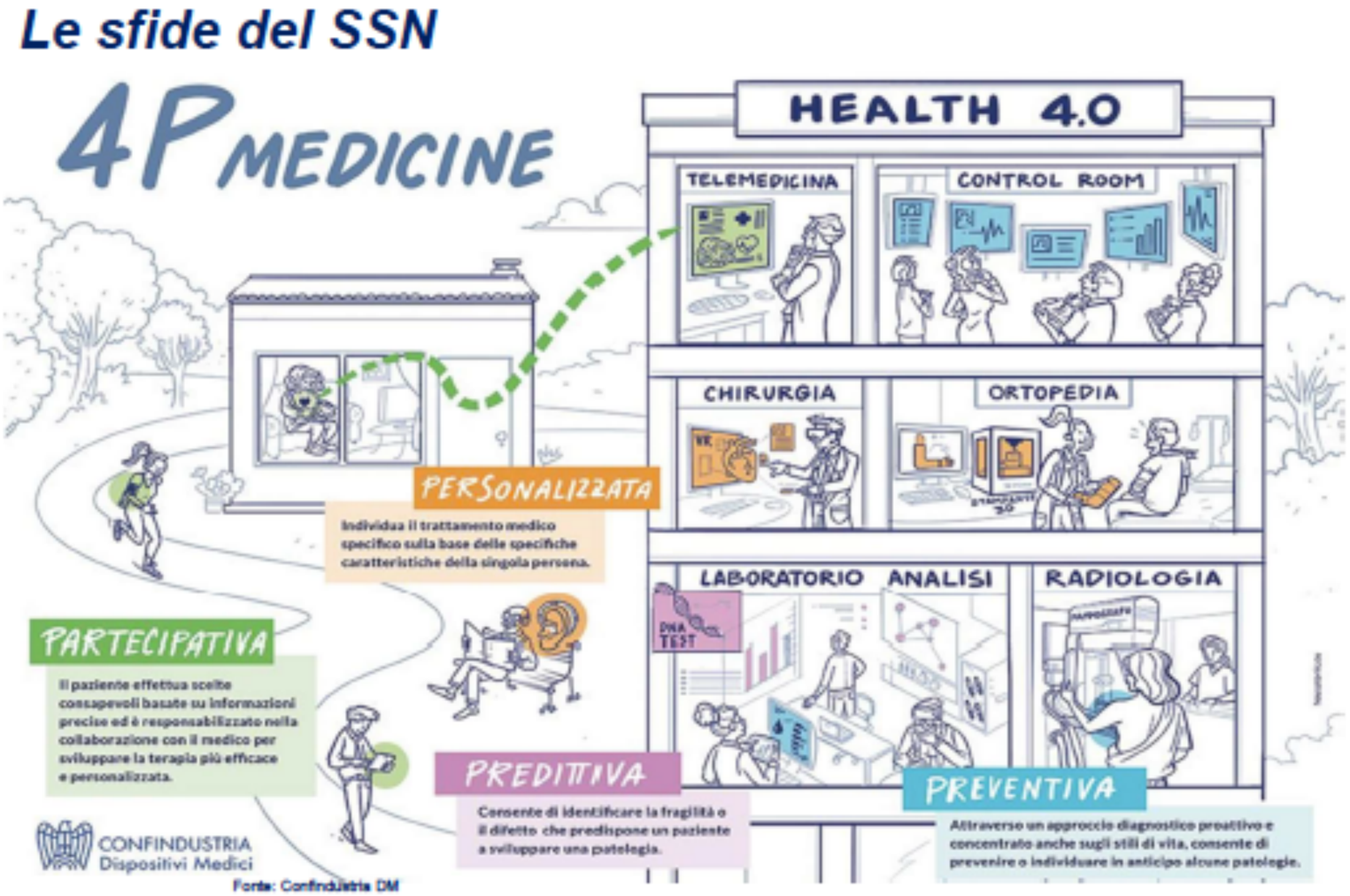
Sostenibilità e governance

Equità di accesso

PREVENZIONE E PROMOZIONE DELLA SALUTE

Fonte: Ministero della Salute 2018

Scenario - E-Health

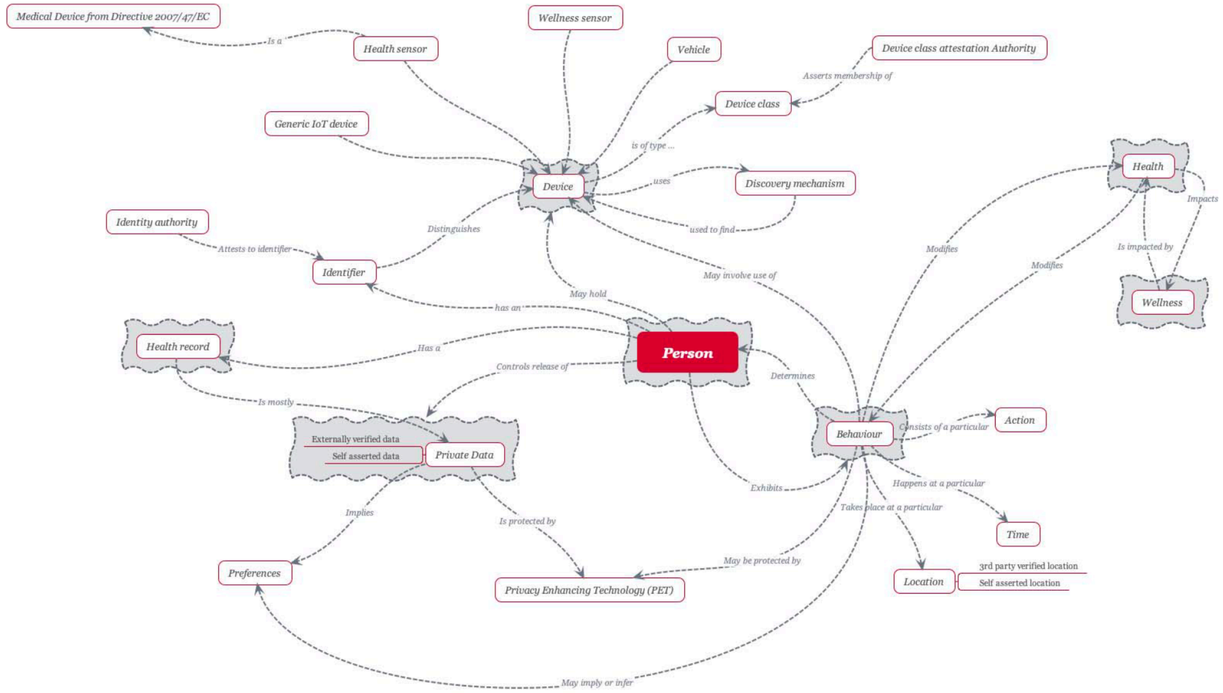


Fonte: Confindustria

Scenario - E-Health

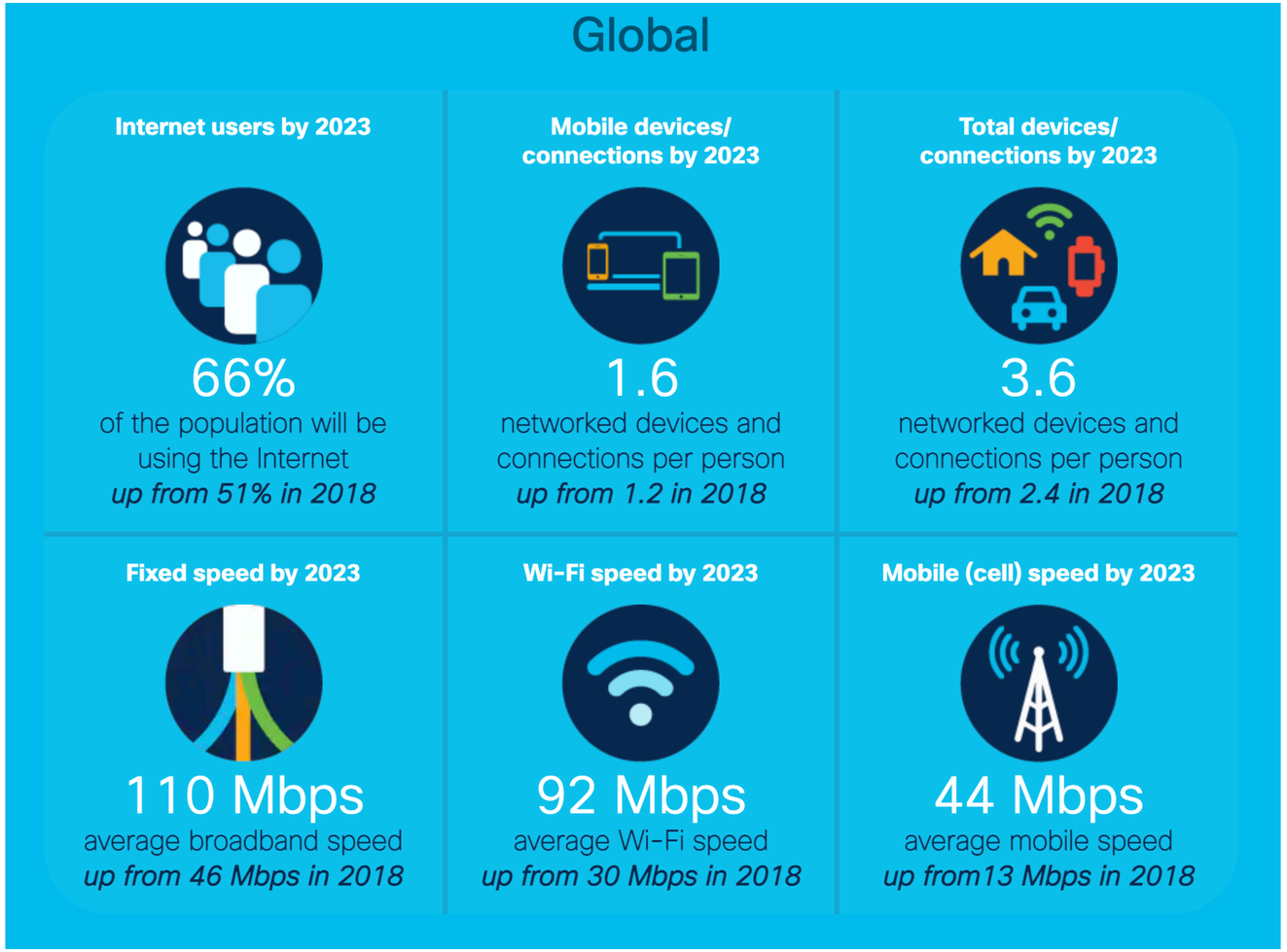
Per “E-Health", o "Sanità in Rete" (o anche Sanità Digitale) s’intende l'utilizzo di strumenti basati sulle tecnologie dell'informazione e della comunicazione per sostenere e promuovere la prevenzione, la diagnosi, il trattamento e il monitoraggio delle malattie e la gestione della salute e dello stile di vita

Objective to meet	Resulting requirement class
A user should expect ubiquitous network connectivity.	Reliability and availability (network interoperability)
The user should reasonably know that eHealth equipment that requires to be connected through a network should be able to access the network.	Availability
The eHealth system should support the interworking of heterogeneous devices and networks.	Network interoperability
An eHealth device should be able interact securely with the eHealth infrastructure.	Security: Availability
Information held within an eHealth device should be protected from unauthorized access, modification and destruction.	Security: Availability; Security: Integrity
Services provided within the eHealth infrastructure should be available only to authorized users of the eHealth system.	Security: Availability (authorization)
Information sent to or from a registered user of the eHealth system should be protected against unauthorized or malicious modification or manipulation during transmission.	Security: Integrity
Information sent to or from a registered user of the eHealth system should not be revealed to any unauthorized 3rd party.	Security: Confidentiality, Security: Availability (Access control); Security: Confidentiality
An eHealth user should be able to communicate confidentially with other users within the eHealth network.	Security: Confidentiality, Privacy
Details relating to the identity of an eHealth user should not be revealed to any unauthorized 3rd party within the eHealth network or in the wider ICT networks.	Security: Availability (Access Control), Security: Availability (Identity Management), Security: Confidentiality, Privacy
Access to the operation of services by authorized eHealth users should not be prevented by malicious activity within the eHealth network or in the wider ICT networks.	Availability
The eHealth system should be able to collect information relating to the context of any eHealth transaction.	See ISG CIM work
The eHealth system and the devices used to access it should allow any member of society to be able to use the system.	Availability



Fonte: ETSI TR 103 477 V1.2.1 (2020-08) eHEALTH;
Standardization use cases for eHealth

Scenario Globale IT



> Opportunità

> Rischi

Fonte: Cisco Global Digital report 2018-2023

Scenario Minacce IT

Le minacce

https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2020

Fonte: Sinibaldi A.; La sicurezza informatica nella PP.AA. - AgID Corso Pilota per RTD - AgID 2020

Scenario - IoT e Ubiquitous Computing

…e smart health???

Fonte: Ivaldi L.; IoT e Sicurezza: le sfide - Seminario CLUSIT 2020

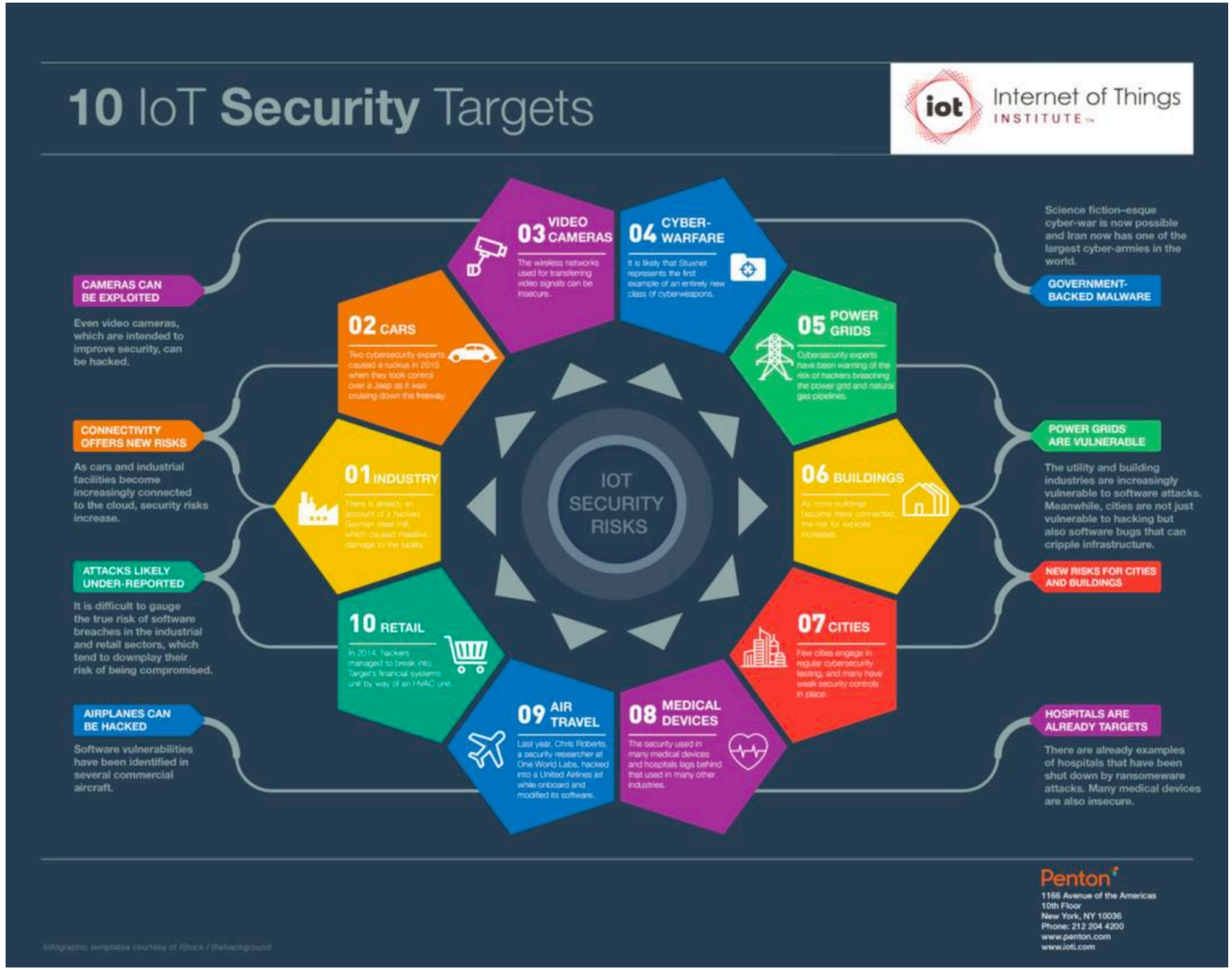
Scenario - IoT

Technology	Definition	Examples
Sensors	A device that generates an electronic signal from a physical condition or event	The cost of an accelerometer has fallen to 40 cents from $2 in 2006.[2] Similar trends have made other types of sensors small, inexpensive, and robust enough to create information from everything from fetal heartbeats via conductive fabric in the mother's clothing to jet engines roaring at 35,000 feet.[3]
Networks	A mechanism for communicating an electronic signal	Wireless networking technologies can deliver bandwidths of 300 megabits per second (Mbps) to 1 gigabit per second (Gbps) with near-ubiquitous coverage.[4]
Standards	Commonly accepted prohibitions or prescriptions for action	Technical standards enable processing of data and allow for interoperability of aggregated data sets. In the near future, we could see mandates from industry consortia and/or standards bodies related to technical and regulatory IoT standards.
Augmented intelligence	Analytical tools that improve the ability to describe, predict, and exploit relationships among phenomena	Petabyte-sized (10^{15} bytes, or 1,000 terabytes) databases can now be searched and analyzed, even when populated with unstructured (for example, text or video) data sets.[5] Software that learns might substitute for human analysis and judgment in a few situations.
Augmented behavior	Technologies and techniques that improve compliance with prescribed action	***Machine-to-machine*** interfaces are removing reliably fallible human intervention into otherwise optimized processes. Insights into human cognitive biases are making prescriptions for action based on augmented intelligence more effective and reliable.[6]

Source: Deloitte analysis.

Fonte: Report Deloitte 2017

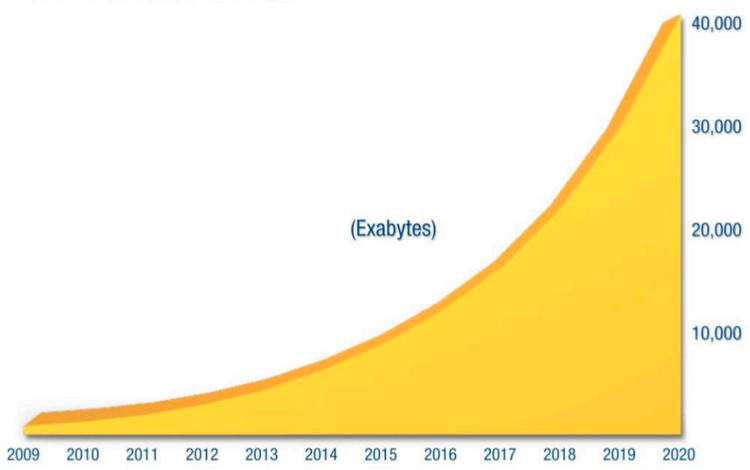
Scenario - IoT

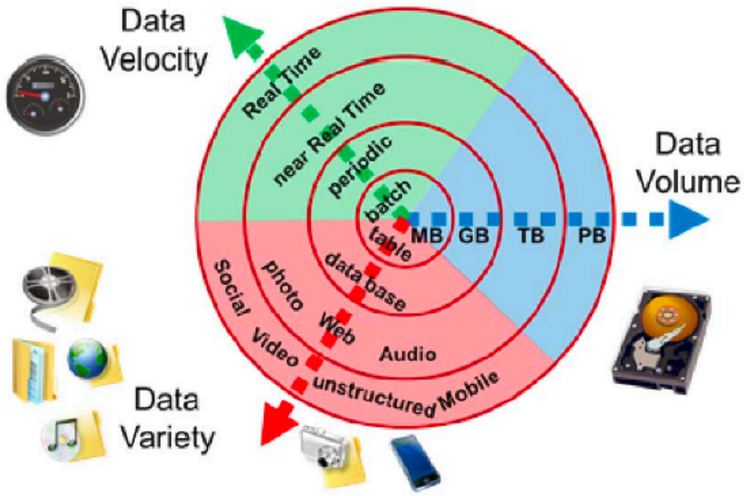


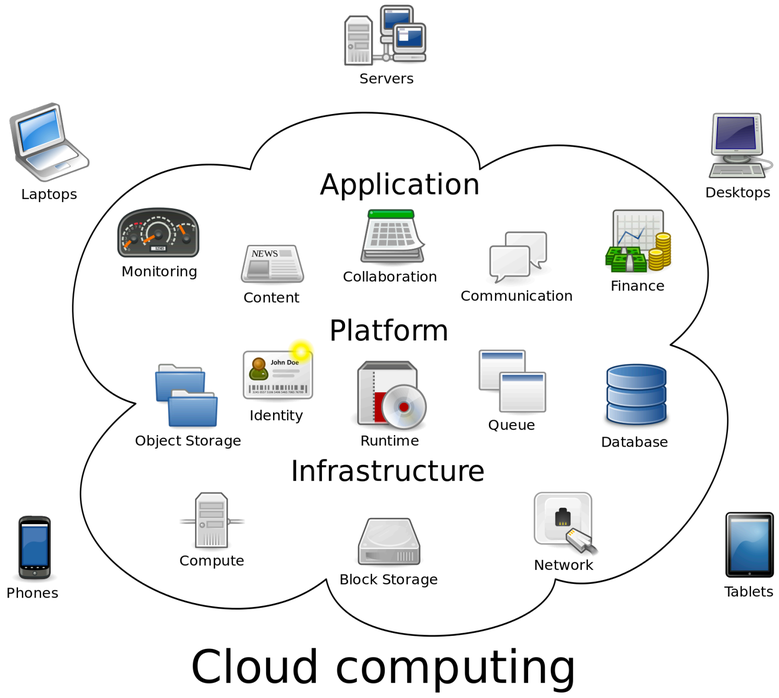
d20… come in D&D

Fonte: Ivaldi L.; cit., 2020

Scenario - Cloud e Big Data

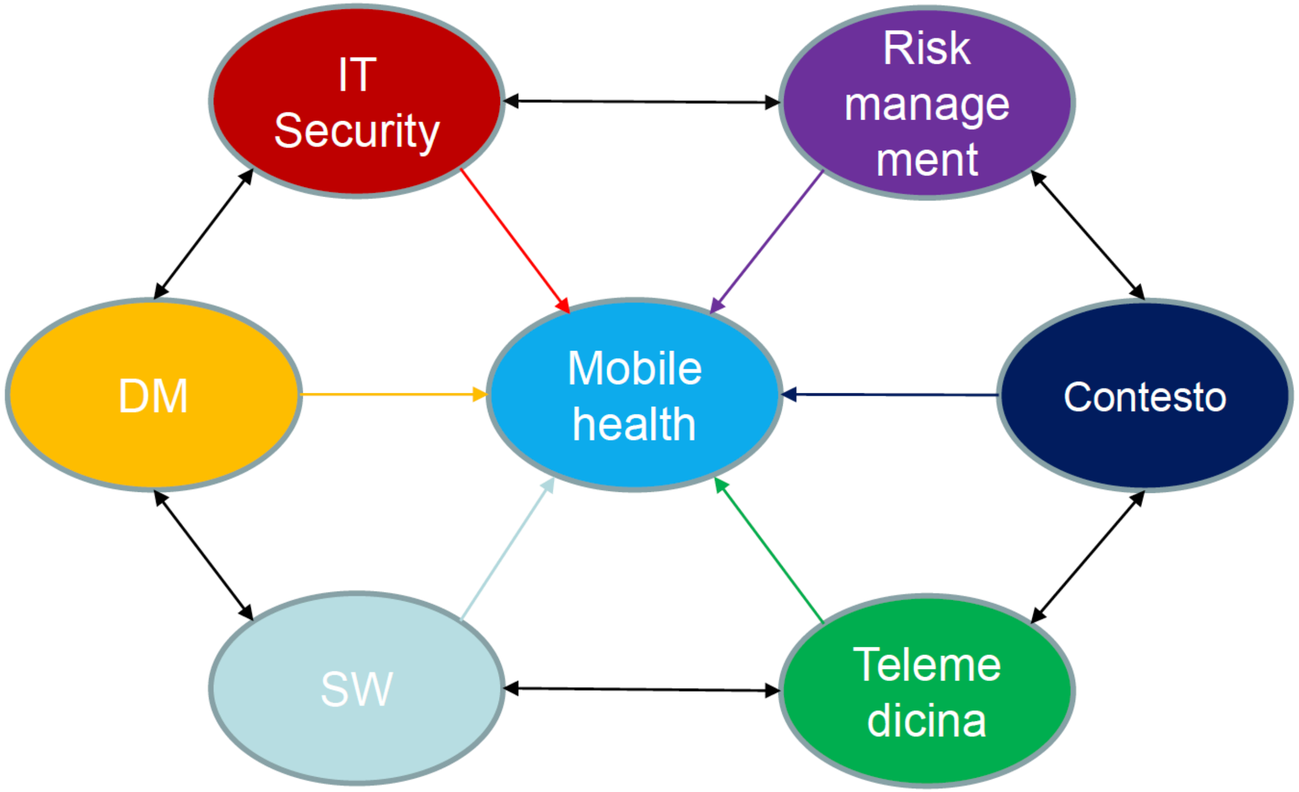


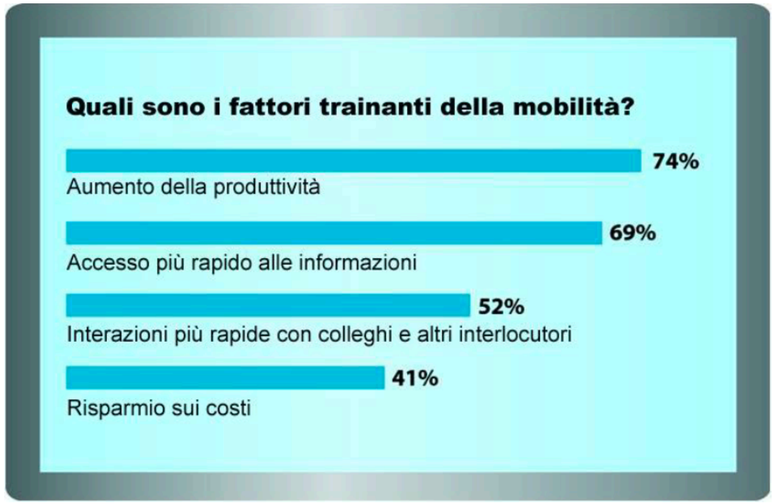




Fonte: Wikipedia 2020

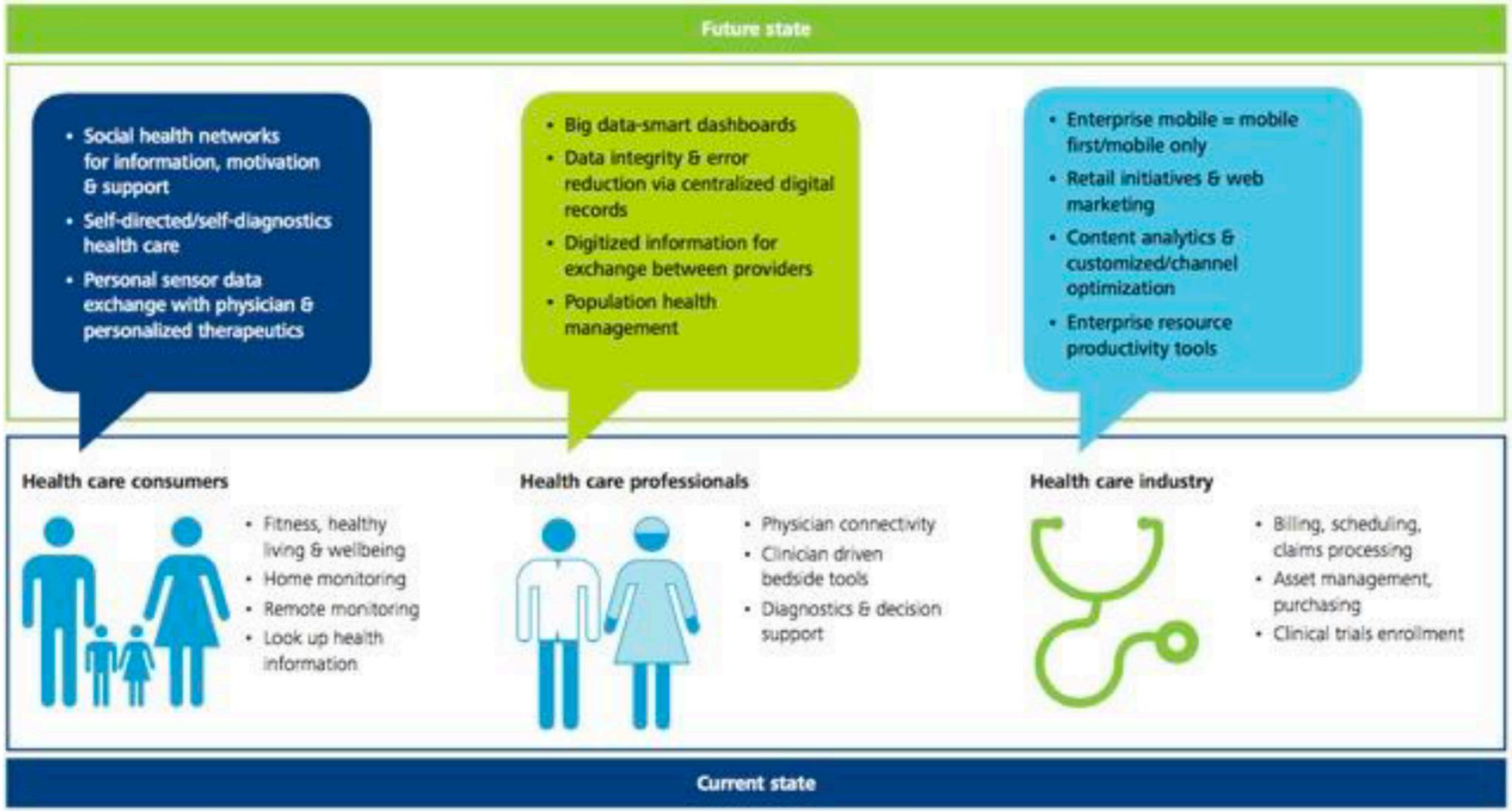
Scenario - mHealth





Fonte: Piaser P.; Mobile-health tra rischi e benefici: proposta di un metodo per la valutazione e l'uso sicuro di tecnologie del mobile in contesti sanitari, A.A. 2013/2014.

Scenario - mHealth (OMS)



Fonte: Piaser P.; cit., 2014

Scenario - mHealth

- **Ma quali rischi?**
  - La sicurezza di dati (privacy) ed informazioni (security)
  - La sicurezza e le performance delle infrastrutture di rete (o del wi-fi/mobile: -mancanza di connettività; -riduzione di banda; -scarsa copertura)
  - Il rischio clinico e di contaminazione
  - Le problematiche di tipo energetico (già viste per l'IoT)
  - Le interferenze EM (sia nell'utilizzo del DM o dell'app in un ambito sanitario sia, viceversa, nell'utilizzo di un DM o di un SW DM in un ambito esterno, ovvero in un contesto non espressamente sanitario)
  - La mobilità (o meglio l'effettiva raggiungibilità e affidabilità d'uso in condizioni di mobilità)
  - Gli standard (o meglio la mancanza di standard che armonizzino o omogeneizzino la situazione complessa relativa a diversi DM, piattaforme, tecnologie, ecc… che hanno ognuna una loro certificazione ma l'insieme non costituiscono ancora un unicum certificato, standardizzato o normalizzato
  - La distrazione ("referto in barca a vela" o "mentre faccio la spesa al supermercato con la moglie…." - utilizzo in contesti rumorosi, luminosi, inappropriati, ecc…)

Fonte: Piaser P.; cit., 2014

Parte 1.2

strumenti (organizzativi), normative, norme tecniche, linee guida

Norme, standard, regolamenti, direttive, linee guida

- **Medical Device Regulation (MDR) (UE) 2017/745**
- **In Vitro Diagnostc Regulation (IVDR) (UE) 2017/746**
- **ISO 14971:2019 Medical Devices - Application of Risk Management to Medical Devices**
- IEC 62304:2006 Medical Device Software - Software Lifecycle Processes
- ISO 31000:2018 Risk Management - Guidelines
- **EN ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems (ISMS) — Requirements**
- ISO/IEC 27001:2018 Information Technology – Security techniques – Information Security management Systems – Overview and vocabulary
- EN ISO/IEC 60601-1-x
- **IEC 82304-1 Health Software Part 1: General requirements for Product Safety**
- **ISO/IEC 80001-1:2010 Application of Risk Management for IT networks Incorporating Medical Devices - Part 1: Roles, Responsibilities and Activities**
- ISO/IEC 80001-5-1 Application of Risk Management for IT networks incorporating medical device – Safety, effectiveness and security in the implementation and use of connected medical devices or connected health software – Part 5-1: Activities in the product life-cycle.
- IEC/TR 80001-2-2 Application of Risk Management for IT networks Incorporating Medical Devices Part 2-2: Guidance for the Disclosure and Communication of Medical Device Security Needs, Risks and Controls

Norme, standard, regolamenti, direttive, linee guida

- IEC/TR 80001-2-8 Application of risk management for IT-networks incorporating medical devices – Part 2-8: Application guidance – Guidance on standards for establishing the security capabilities identified in IEC TR 80001-2-2
- ISO/IEC 80001-xx including IEC/TR 80001-2-1, IEC/TR 80001-2-3, IEC/TR 80001-2-4, IEC/TR 80001-2-5, ISO/TR 80001-2-6, ISO/TR 80001-2-7 or other
- EN ISO 62366 / ISO 60601-4 Usability Engineering
- IEC 62443-x-x Industrial Cybersecurity Lifecycle
- IEC 62443-4-2 Security for industrial automation and control systems. Part 4-2: Technical security requirements for IACS components.
- IEC 62443-4-1 Security for industrial automation and control systems. Part 4-1: Secure product development lifecycle requirements.
- IEC/TR 60601-4-5 Medical Electrical Equipment – Part 4-5. Safety related technical security specifications for medical devices.
- ISO 27799:2016 Health informatics — Information security management in health using ISO/IEC 27002
- ISO/IEC 20000-1:2011 Information Technology - Service management system requirements
- **ISO/IEC 27701:2019 Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines**
- ISO 13485:2016 Medical Devices - Quality Management Systems - Requirements for Regulatory Purposes
- Direttiva NIS (UE) 2016/1148 recepita con D.Lgs. 65/2018
- **General Data Protection Regulation (GDPR) (UE) 2016/679 recepito con D.Lgs. 101/2018**
- **“Cybersecurity Act” - Regolamento (UE) 2019/881**

Norme, standard, regolamenti, direttive, linee guida

- **Guida Tecnica CEI 62-237 “Guida alla gestione del software e delle reti IT-medicali nel contesto sanitario. Parte 1: gestione del software”**
- NIST Cybersecurity Framework
- IoT Cybersecurity Improvement Act of 2020 (US)
- CSC - ABSC e Misure Minime di Sicurezza AGID 2017
- EN 303 645 ETSI v. 2.1.1
- MEDDEV 2.X/Y (0<X<16 , 0<Y<10)
- ISO/IEC 22301:2019 e ISO/IEC 27031:2011 per la Continuità Operativa (BC)
- **MDCG 2019-16 Guidance on Cybersecurity for medical devices - Medical Devices Coordination Group (MDCG) Document - December 2019 (July 2020 rev. 1)**
- MDCG 2020-1 Guidance on Clinical Evaluation (MDR) / Performance Evaluation (IVDR) of Medical Device Software - Medical Devices Coordination Group (MDCG) Document - March 2020
- CAD - Codice dell’Amministrazione Digitale D.Lgs. 82/05 e s.m. e i.
- Testo unico sulla salute e sicurezza sul lavoro D.Lgs. 81/08 e s.m. e i.
- ETSI TR 103 477 V1.2.1 (2020-08) eHEALTH - Standardization use cases for eHealth
- ISO 25237:2017 Health informatics — Pseudonymization

Norme, standard, regolamenti, direttive, linee guida

- **Linea Guida AgID - La sicurezza nel Procurement ICT - 2020**
- **Linea Guida AgID - Sviluppo del software sicuro - 2020**
- **Piano triennale per l’informatica nella PA 2020-2022**
- Raccomandazioni AgID - TLS e cipher suite
- ISO/IEC 31010:2019 - Risk management — Risk assessment techniques
- ISO/IEC 27005:2018 - Information technology — Security techniques — Information security risk management
- ISO/IEC 27002:2013 - Information technology — Security techniques — Code of practice for information security controls
- ISO/IEC 29100:2011- Information technology — Security techniques — Privacy framework
- ISO/IEC 27018:2019 - Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
- Linee Guida AgID - caratterizzazione dei sistemi cloud per la PA
- ISO/IEC 27017 Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services
- ENISA Cloud Security for Healthcare services - 2021
- ENISA Procurement guidelines for cybersecurity in hospitals - 2020
- Framework Nazionale per la Cyber Security e la Data Protection - CIS sapienza - CINI -2019

IT e DM - Standard tecnici e normativi

CEI 62-237: SOFTWARE AND MEDICAL IT-NETWORKS MANAGEMENT GUIDE IN HEALTHCARE

IEC 80001-1:2010: APPLICATION OF RISK MANAGEMENT FOR IT-NETWORKS INCORPORATING MEDICAL DEVICE

CEI UNI EN ISO 14971: MEDICAL DEVICES - APPLICATION OF RISK MANAGEMENT TO MEDICAL DEVICES

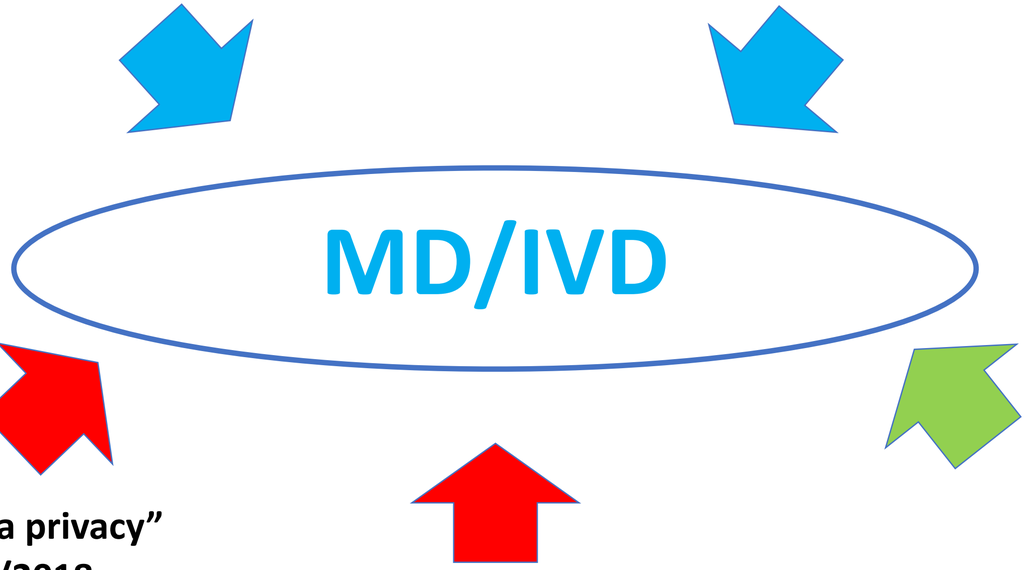
UNI ISO 31000: RISK MANAGEMENT;
EN ISO/IEC 60601-1-x

ISO IEC 27001: INFORMATION SECURITY MANAGEMENT SYSTEMS;
IEC 62304:2006 Medical Device Software - Software Lifecycle Processes;
NIST Cybersecurity Framework;

IT e DM - Regolamenti, leggi, linee guida nazionali e europei

UE 2017/745 MDR e EU 2017/746 IVDR

Linee Guida MEDDEV 2.X/Y (0<X<16 , 0<Y<10);
Linee Guida MDCG



D.Lgs 196/2003 “Codice della privacy” novellato da D. Lgs. 101/2018

GDPR – Regolamento UE 2016/679;
UE 2019/881 CYBERSECURITY ACT;
Direttiva NIS “Network and Information Security” (UE) 2016/1148 recepita con D.Lgs. 65/2018

AGID: Misure Minime per la Sicurezza della PA;
Piano Triennale per l’informatica nella PA 2020-2022;
Garante della Privacy;
CERT-AgID

DM - Regolamenti UE 2017/745 e UE 2017/746

Le finalità del nuovo Regolamento: migliorare la sicurezza e la salute

Stabilire un quadro normativo **solido, trasparente, prevedibile** e **sostenibile** per i dispositivi medici, che garantisca un livello elevato di sicurezza e di salute sostenendo nel contempo l'innovazione.

Al fine di migliorare la salute e la sicurezza è opportuno rafforzare profondamente alcuni elementi chiave dell'attuale approccio normativo, quali il **controllo degli organismi notificati**, le procedure di **valutazione della conformità**, le **indagini cliniche** e la **valutazione clinica**, la **vigilanza e la sorveglianza** del mercato, e introdurre nel contempo disposizioni che garantiscano la **trasparenza** e la **tracciabilità** dei dispositivi.

Molti degli **obblighi dei fabbricanti**, come quelli relativi alla valutazione clinica o alle segnalazioni nel quadro della vigilanza, che nella Direttiva erano definiti solo negli allegati, sono stati **integrati nel dispositivo del Regolamento** per facilitarne l'attuazione.

Fonte: Leone M.G.; I dispositivi medici: aspetti generali e nuovo regolamento. Ministero della Salute, 2021

DM - Regolamenti UE 2017/745 e UE 2017/746

1. **Migliore protezione della salute e della sicurezza del paziente:**
   - ✓ **Controllo pre-mercato dei dispositivi ad alto rischio rafforzato** con il convolgimento di panels di esperti a livello Europeo
   - ✓ Inclusione di **alcuni dispositivi estetici nello scopo** di applicazione
   - ✓ **Requisiti minimi Europei per il "reprocessing"** dei dispositivi a uso singolo
   - ✓ Rafforzamento del **processo di designazione e controllo degli organismi notificati**
   - ✓ Rafforzamento delle regole sulla **valutazione clinica** e sulle **indagini cliniche**
   - ✓ Regole più stringenti per i **dispositivi composti di sostanze**
   - ✓ **Nuove regole dedicate a software, apps e nanomateriali**
   - ✓ **Nuovo sistema di classificazione per i diagnostici *in vitro*** basato sui principi internazionali (80% di questi dispositivi saranno controllati da un organismo notificato)
   - ✓ Regole più rigide per **l'uso di sostanze pericolose** in certi dispositivi
   - ✓ Introduzione di un **sistema UDI**
   - ✓ **Responsabilità dei produttori/fabbricanti**

DM - Regolamenti UE 2017/745 e UE 2017/746

2.Maggiore certezza legale e supporto all'innovazione

- ✓Uso del Regolamento Europeo come **strumento legislativo**
- ✓**Chiarimento dello scopo di applicazione** per MD e IVD
- ✓Ruolo più incisivo della Commissione nel contesto di **decisioni sullo *status* regolamentare di un prodotto**
- ✓Chiarimento sul regime applicabile alla fabbricazione di **dispositivi "in-house"**
- ✓Chiarimento del **ruolo e delle responsabilità degli operatori economici**
- ✓Nuove regole dedicate per **software medici e apps medici**

3.Maggiore trasparenza e responsabilizzazione del paziente

- ✓Creazione di un **database Europeo sui dispositivi medici** (EUDAMED) con larga parte dell'informazione accessibile al pubblico
- ✓Introduzione di una **"carta d'impianto"** a livello Europeo
- ✓**Riassunto della sicurezza e della performance clinica** per tutti i dispositivi Classe III e impiantabili da introdurre in EUDAMED
- ✓Nuovi obblighi per fabbricanti e mandatari, allo scopo di **proteggere i pazienti danneggiati**

DM - Regolamenti UE 2017/745 e UE 2017/746

4. **Approccio maggiormente Europeo**
   - ✓ **Registrazione dei dispositivi e operatori** a livello Europeo (EUDAMED)
   - ✓ **Rafforzamento della cooperazione tra Stati** in materia di vigilanza e sorveglianza di mercato
   - ✓ Istituzione del **Gruppo di coordinamento (MDCG)**, cuore della gestione delle future normative
   - ✓ Consolidamento e rafforzamento della procedura del **controllo incrociato degli organismi Notificati**
   - ✓ Introduzione di una **verifica coordinata per le indagini cliniche** che si svolgono in piu di uno Stato membro
     - **Alcune (…) criticità**
   - ✓ **Costi per le aziende (indagini cliniche, personale, tempi di progettazione, sviluppo…)**
   - ✓ **Prodotti borderline (DM a base di sostanze vs medicinali) MEDDEV 2.1/3 rev3: la modifica proposta relativa alla azione farmacologica introducendo il generico termine “interaction” farebbe di tutti i DM a base di sostanze dei medicinali….**

DM - Regolamenti UE 2017/745 e UE 2017/746

I cardini del processo rimangono gli stessi

Dall'idea al mercato

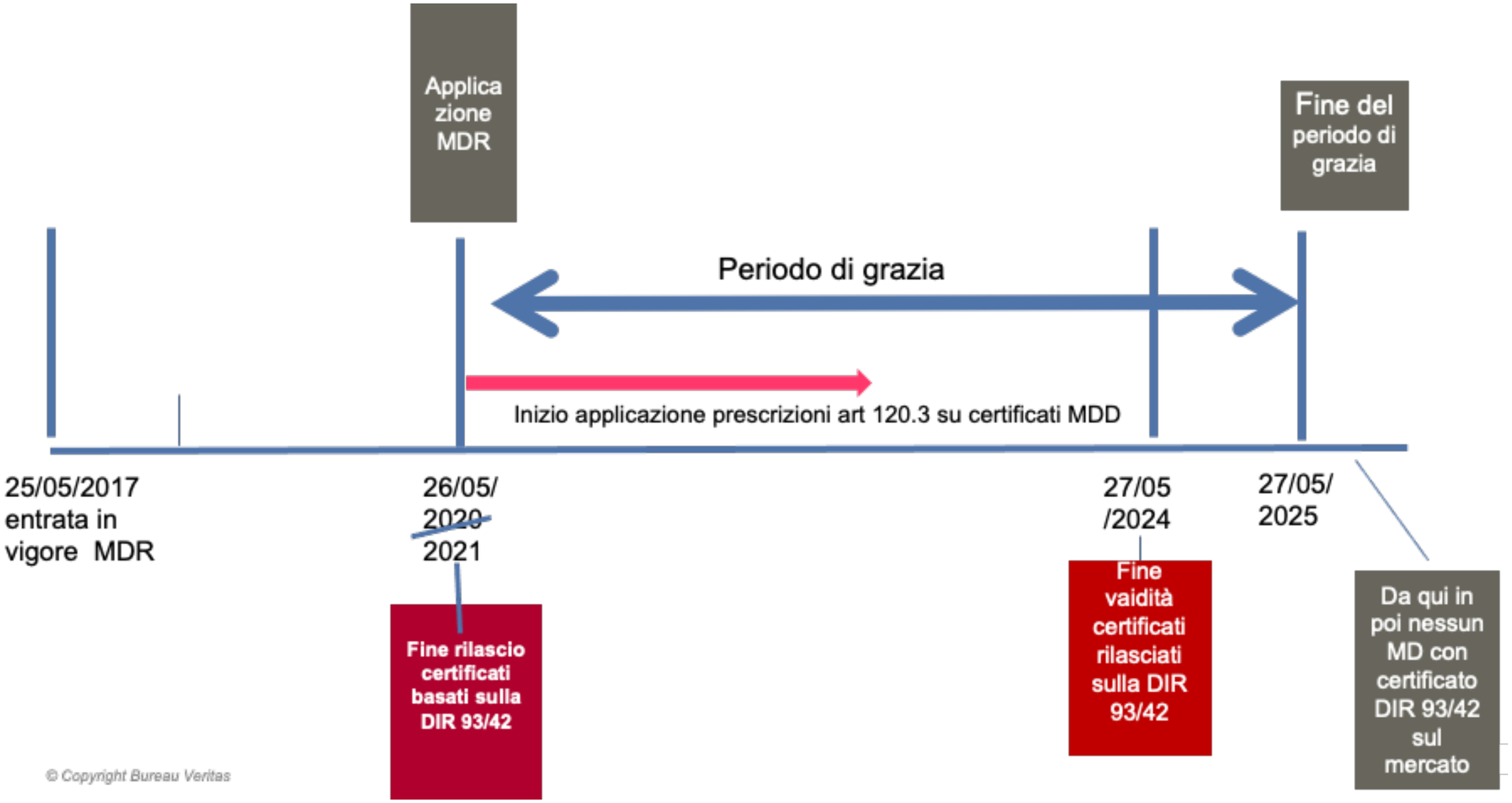
Ricerca & Sviluppo

- Qualifica e **classificazione** del dispositivo (Art. 51 e All.VIII)
- Rispetto dei **requisiti generali di prestazione e sicurezza** (All. I), applicando norme tecniche armonizzate/specifiche comuni
- Implementare un sistema di **gestione dei rischi** (All. I) e della **qualità**
- Predisposizione **documentazione tecnica** (All. II, III), incluse etichette ed IFU
- Registrazione **fabbricante** in **EUDAMED** (Art. 31)

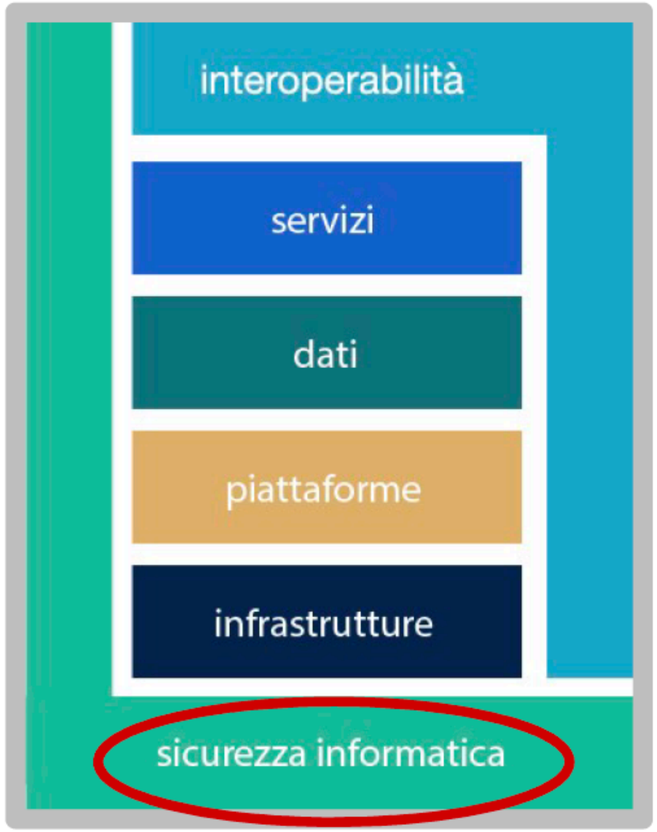
CONFINDUSTRIA Dispositivi Medici

Fonte: Capece Minutolo F.;
L'industria italiana dei dispositivi medici nel passaggio dalle Direttive al nuovo Regolamento. Confindustria, 2021

DM - Regolamenti UE 2017/745 e UE 2017/746



IT - Piano Nazionale per l'informatica della PA



IMPOSTAZIONE DEL PIANO

- **Semplificazione** della struttura del documento e dei capitoli
- Particolare rilevanza per **le azioni specifiche** da porre in essere da parte delle PA

Circa **100 azioni nel triennio a carico delle PA** con focus e indicazioni specifiche sulle azioni delle **PA.**

EFFICACIA DEL PIANO

- Valorizzazione della trasversalità delle componenti interoperabilità **e sicurezza informatica**
- Evidenziazione degli **aspetti organizzativi** necessari al completamento del percorso di trasformazione digitale delle PA

MONITORAGGIO DEL PIANO

- Introduzione di un approccio orientato alla misurazione dei risultati
- Individuazione di un percorso operativo che coinvolga le PA nell'attività di monitoraggio del Piano

Fonte: Rossi M.;
Strumenti di prevenzione per la sicurezza informatica - AgID corso pilota per RTD - 2020

IT - Piano Nazionale per l'informatica della PA

La sicurezza nel Piano triennale 2020 – 2022

L' esigenza per la PA di contrastare le minacce cibernetiche è fondamentale in quanto garantisce non solo la disponibilità, l'integrità e la riservatezza delle informazioni proprie del Sistema informativo della Pubblica Amministrazione, ma è il presupposto per la protezione del dato che ha come conseguenza diretta l'aumento della fiducia nei servizi digitali erogati dalla PA.

OBIETTIVI DEL Cap. 6	RISULTATI ATTESI
1 Aumentare la **consapevolezza del rischio cyber** (Cyber Security Awareness) nelle PA	❑ Incremento del livello di Cyber Security Awareness nella PA
2 Aumentare il livello di **sicurezza informatica dei portali istituzionali** della Pubblica Amministrazione	❑ Incremento del numero dei portali istituzionali che utilizzano il protocollo HTTPS only ❑ Massimizzazione del numero dei Content Management System (CMS) non vulnerabili utilizzati nei portali istituzionali delle PA

Fonte: Rossi M.; cit., 2020

Tool di Cyber Risk Management - Quadro d'insieme

Il tool nasce per supportate le PA nel self-assessment di sicurezza informatica e migliorare la consapevolezza sulle materie di Cyber Security e permette di valutare le vulnerabilità e il livello di esposizione al rischio
Il tool è *web based* e l'accesso per le PA avviene attraverso SPID.

COME FUNZIONA IL TOOL?

FASE INIZIALE

Definizione del contesto in cui opera la PA

FASE DI ANALISI

- ❑ Identificazione dei rischi
- ❑ Simulazione degli effetti di mitigazione delle azioni
- ❑ Piano dei trattamenti

FASE OPERATIVA

VALUTAZIONE DELLE AZIONI DA METTERE IN CAMPO Orizzontale su tutta la PA o su singoli servizi

LA DIFFUSIONE DEL TOOL

UNIONE EUROPEA
Fondo sociale europeo
Fondo Europeo di Sviluppo Regionale

Agenzia per la Coesione Territoriale

Dipartimento della Funzione Pubblica

PON GOVERNANCE E CAPACITÀ ISTITUZIONALE 2014-2020

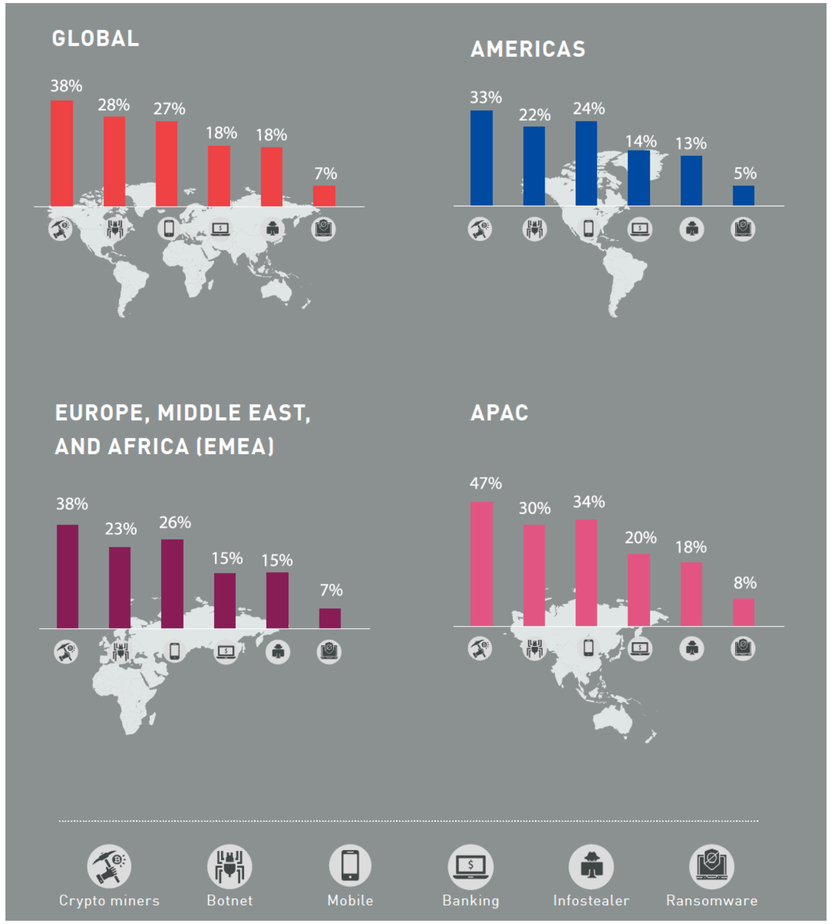
Fonte: Rossi M.; cit., 2020

IT - Cybersecurity (Rapporto CLUSIT e Checkpoint 2020)

Con la popolarità del **cloud computing** e degli **smartphone** connessi in rete, non è un segreto che ci sono più modi per colpire un'organizzazione. Quello che una volta era un perimetro di rete sicuro, è ora offuscato, frammentato e permeabile agli attacchi informatici cosa che i malintenzionati sanno bene. Se c'è un chiaro risultato dal 2019, è che nessuna organizzazione, grande o piccola, è immune da quelli che possono essere dei devastanti cyber-attacchi. Gli exploit sono più sofisticati, difficili da individuare e mirati più che mai. Con tassi di criminalità informatica che si stima abbiano generato 1,5 miliardi di dollari nel 2018, navigare nel complesso panorama delle minacce informatiche di oggi richiede una cybersicurezza completa.

VITTIME PER TIPOLOGIA	2014	2015	2016	2017	2018	2019	2019 su 2018	Trend
Gov - Mil - LEAs - Intel	213	223	220	179	252	203	-19.4%	↓
Multiple targets	-	-	49	222	304	395	29.9%	↑
Healthcare	32	36	73	80	159	186	17.0%	↑
Banking / Finance	50	64	105	117	156	141	-10.2%	↘
Online Services / Cloud	103	187	179	95	129	247	91.5%	↑
Research - Education	54	82	55	71	110	100	-8.3%	↘
Software / Hardware Vendor	44	55	56	68	109	83	-23.9%	↓
Entertainment / News	77	138	131	115	102	70	-31.4%	↓
Critical Infrastructures	13	33	38	40	57	37	-35.1%	↓
Hospitability	-	39	33	34	45	27	-40.0%	↓
GDO / Retail	20	17	29	24	39	50	28.2%	↑
Others	172	51	38	40	30	53	76.7%	↑
Org / ONG	47	46	13	8	18	18	0.0%	-
Gov. Contractors / Consulting	13	8	7	6	14	11	-21.4%	↓
Telco	18	18	14	13	11	17	54.5%	↑
Automotive	3	5	4	4	9	10	11.1%	↗
Security Industry	2	3	0	11	4	17	325.0%	↑
Religion	7	5	6	0	3	3	0.0%	-
Chemical / Medical	5	2	0	0	1	2	100.0%	↑
TOTALE	873	1012	1050	1127	1552	1670		

Fonte: Rapporto CLUSIT 2020



5G
IoT
Cloud
Big Data
Mobile

Fonte: CyberSecurity Report, Checkpoint 2020

Sanità -> tecnologie IT e Biomediche -> cybersicurezza (data (privacy) & system security)
Safety

Cybersecurity - Regolamento UE 2019/881

Cybersecurity Act – UE 2019/881

Rafforzare la resilienza agli attacchi informatici e creare un mercato unico della sicurezza informatica in termini di prodotti, servizi e processi, aumentando la fiducia dei consumatori nelle tecnologie digitali (la nascita di un marchio CE di sicurezza informatica?)

Il ruolo dell'ENISA (Agenzia dell'Unione europea per la sicurezza informatica)

Cybersecurity - Direttiva NIS (UE 2016/1148)

La Direttiva (UE) 2016/1148, conosciuta come Direttiva NIS, è intesa a definire le misure necessarie a conseguire un elevato livello di sicurezza delle reti e dei sistemi informativi.

La Direttiva è stata dall'Italia recepita con Decreto Legislativo 18 maggio 2018, n.65.

Si applica a:

Operatori di Servizi Essenziali (OSE): sono i soggetti, pubblici o privati, che forniscono servizi essenziali per la società e l'economia nei settori sanitario, dell' energia, dei trasporti, bancario, delle infrastrutture dei mercati finanziari, della fornitura e distribuzione di acqua potabile e delle infrastrutture digitali.

Fornitori di Servizi Digitali (FSD): sono le persone giuridiche che forniscono servizi di e-commerce, cloudcomputing o motori di ricerca, con stabilimento principale, sede sociale o rappresentante designato sul territorio nazionale.

OSE e FSD devono **adottare misure tecniche e organizzative adeguate** e proporzionate alla gestione dei rischi e a **prevenire e minimizzare l'impatto degli incidenti a carico delle reti e dei sistemi informativi** e **notificare**, senza ingiustificato ritardo, **gli incidenti** che hanno un impatto rilevante rispettivamente sulla continuità e sulla fornitura del servizio, al CSIRT italiano, informandone anche l'Autorità competente NIS di riferimento.

Cybersecurity (& privacy) - Regolamento UE 2016/679 - GDPR

Principi fondamentali:

Salvaguardare i diritti e le libertà dell'interessato, la dignità umana dell'interessato e gli interessi legittimi e i diritti fondamentali

Accountability: responsabilità del titolare (e dei responsabili/autorizzati al trattamento) (art. 24)

Liceità, correttezza e trasparenza; minimizzazione dei dati (pertinenti e limitati) e accuratezza

Sicurezza dei dati personali (CIA Triad)

Data Protection Impact Analysis (analisi e gestione dei rischi) (art. 35)

Focus sui DATI

Misure tecniche e organizzative adeguate (art. 32)

Registro delle attività di trattamento e del DPO (Artt.30 e 37)

Il GDPR prevede che il titolare del trattamento costruisca una mappa dei rischi che consenta una stima dell'indice di rischio generico per ogni tipologia di trattamento (in sanità di tutti quei trattamenti associati ai DM)

modello integrato di sicurezza + privacy +…. gestione del rischio

Cybersecurity & DM

REQUISITI ESSENZIALI

Allegato I del D. Lgs. 46/97 per i Dispositivi Medici

Allegato 1 del D.Lgs 507/92 per i Dispositivi Medici Impiantabili Attivi

Allegato I
Regolamento UE 2017/745

I requisiti essenziali definiscono regole e principi generali di sicurezza e prestazione, **senza però prescrivere dettagli tecnici per raggiungere l'ottemperanza a tali requisiti**.
I prodotti, al fine dell'apposizione del marchio CE, devono rispettare i requisiti essenziali ad essi applicabili.

Fonte: Leone M.G.; cit., 2021

Cybersecurity & DM

Medical Device

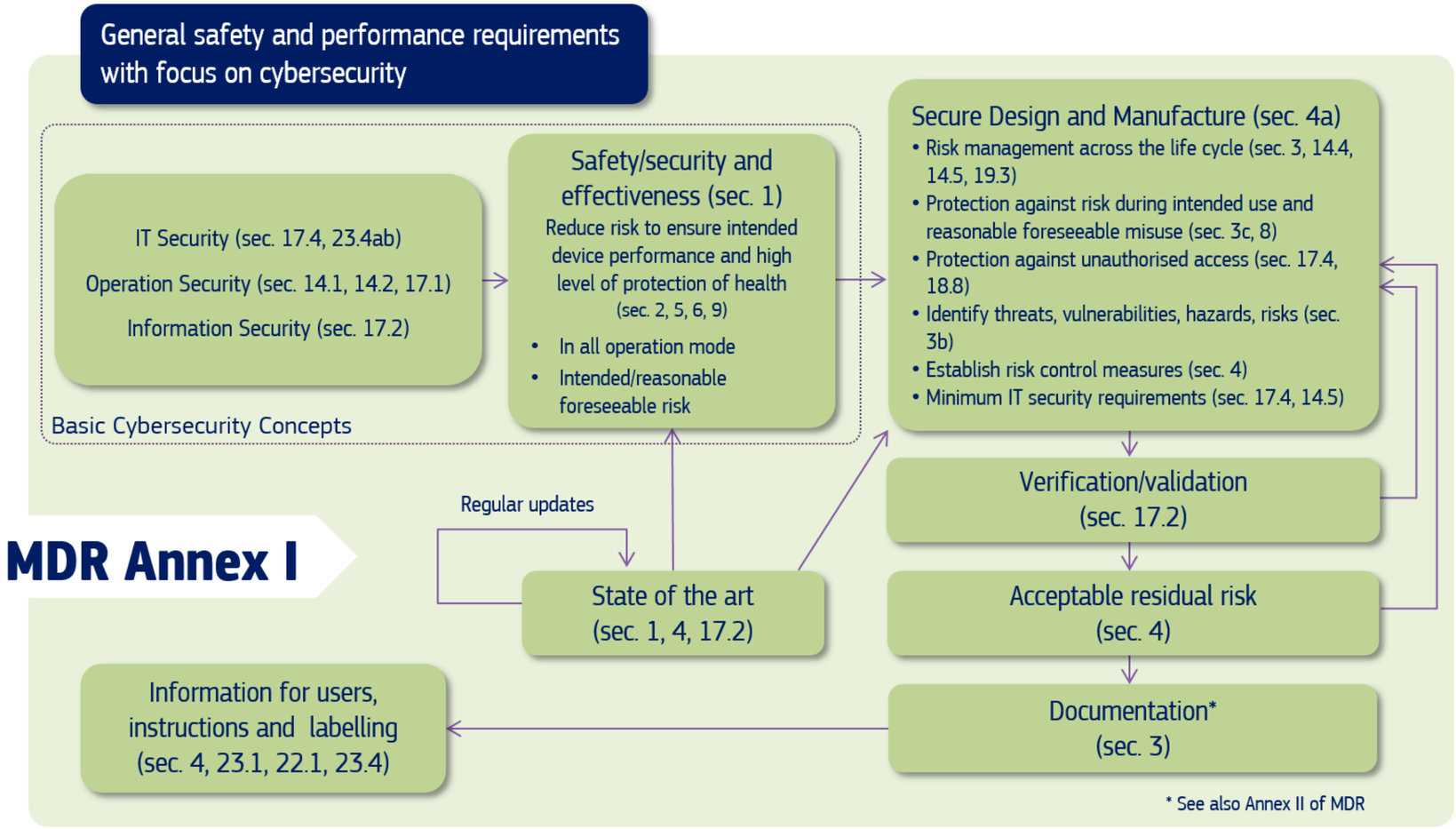
Medical Device Coordination Group Document MDCG 2019-16 rev. 1

MDCG 2019-16
Guidance on Cybersecurity for medical devices

December 2019
July 2020 rev.1

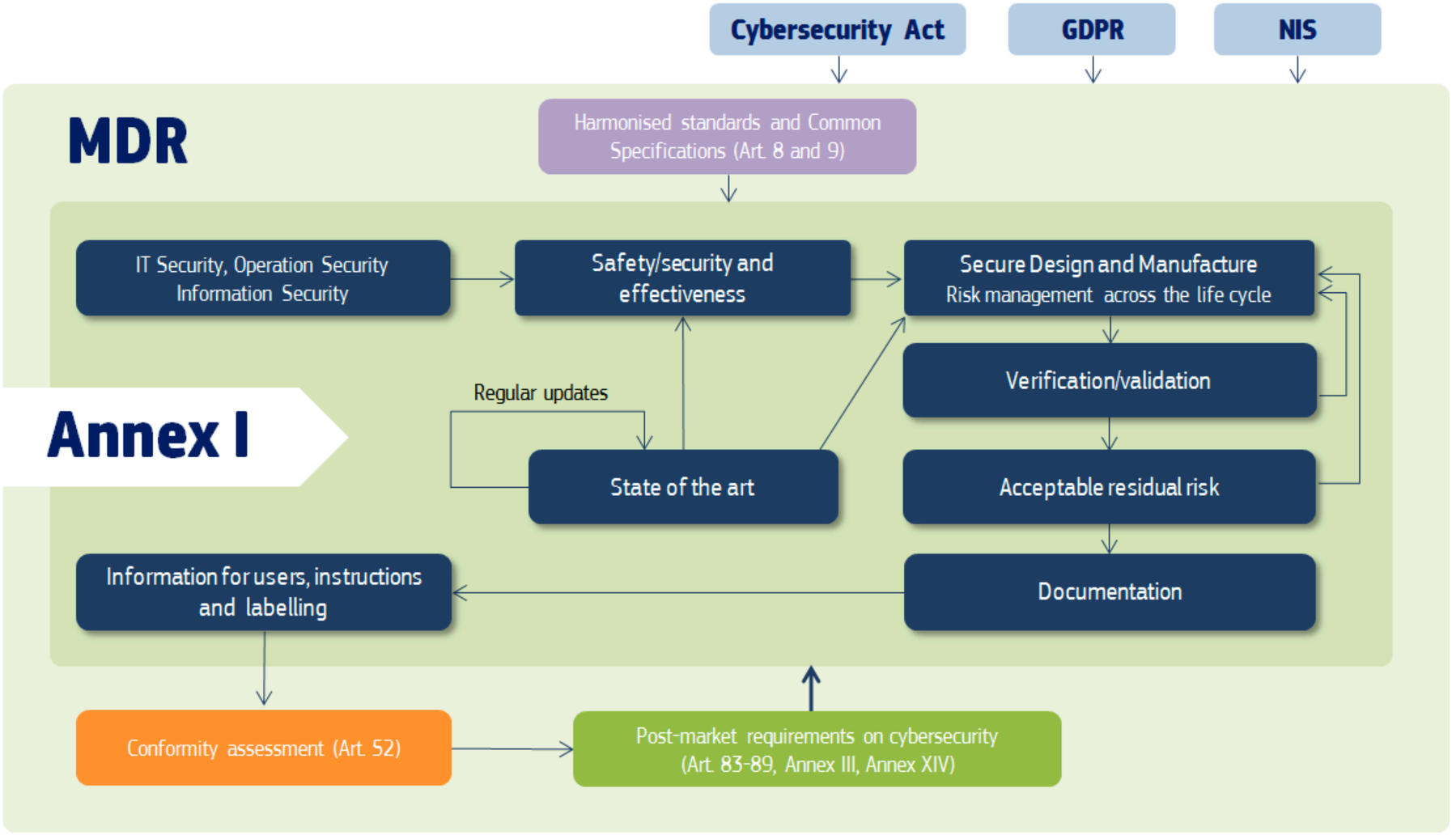
MDCG 2019-16 GUIDANCE ON CYBERSECURITY FOR MEDICAL DEVICES

MDCG 2019-16 GUIDANCE ON CYBERSECURITY FOR MEDICAL DEVICES



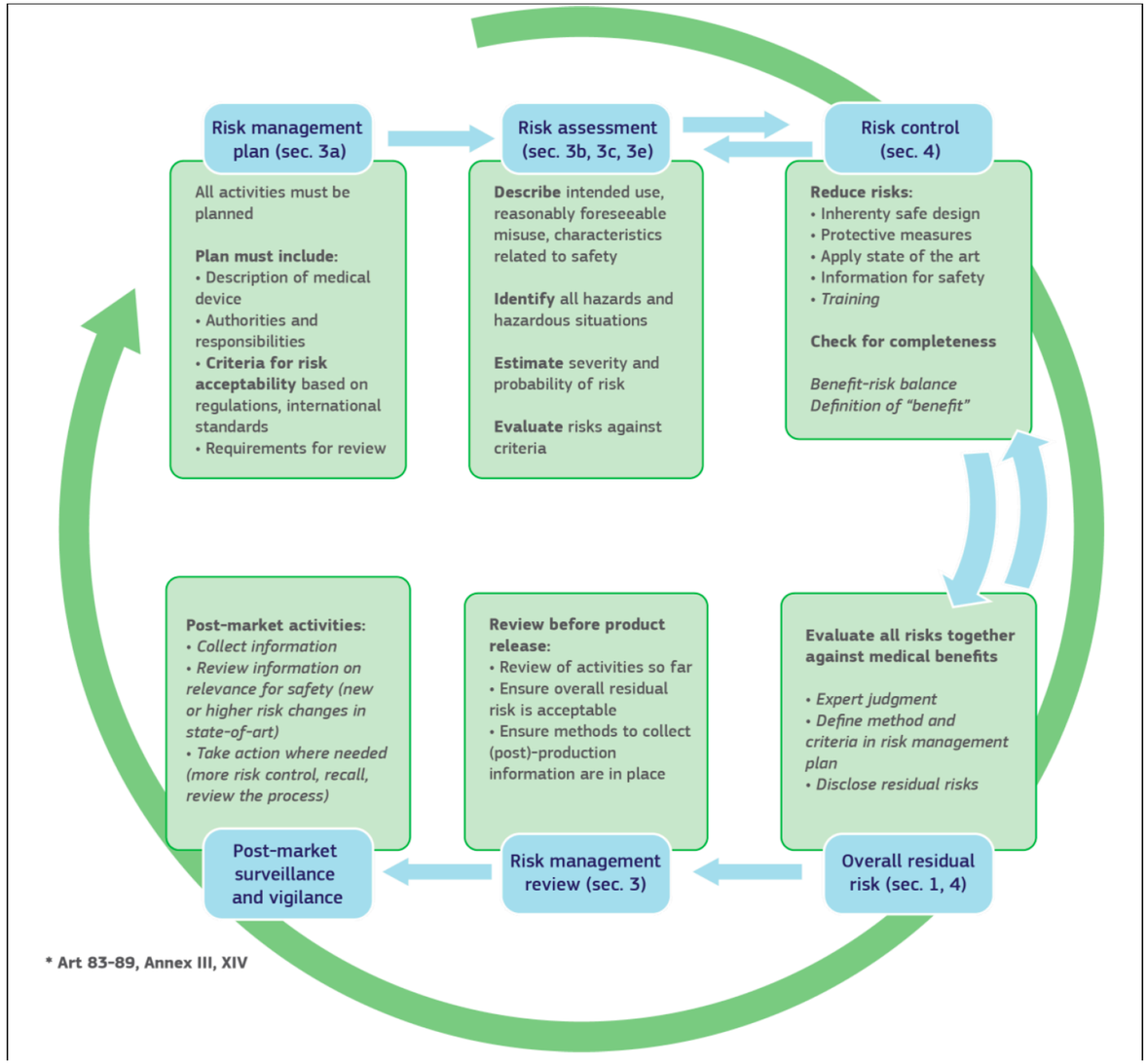
Fonte: MDCG 2019-16 Guidance on Cybersecurity for medical devices - Medical Devices Coordination Group (MDCG) Document - December 2019 (July 2020 rev. 1)

MDCG 2019-16 GUIDANCE ON CYBERSECURITY FOR MEDICAL DEVICES



Fonte: MDCG 2019-16, cit. - December 2019 (July 2020 rev. 1)

MDCG 2019-16 GUIDANCE ON CYBERSECURITY FOR MEDICAL DEVICES



Fonte: MDCG 2019-16, cit. - December 2019 (July 2020 rev. 1)

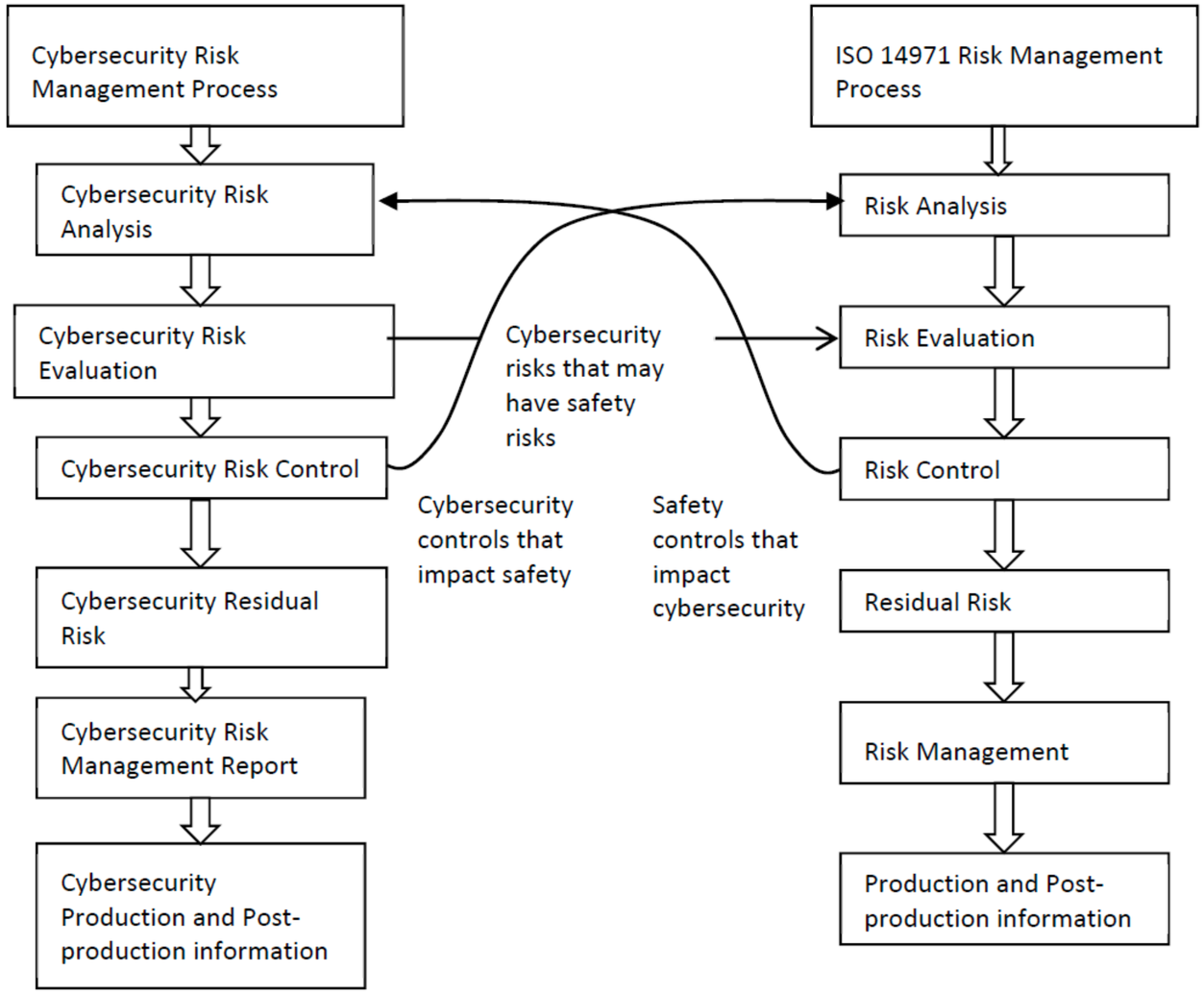
MDCG 2019-16 GUIDANCE ON CYBERSECURITY FOR MEDICAL DEVICES

The list of known vulnerabilities and attack vectors is the basis for specifying the **security capabilities**, depending on the risk management, required for appropriate protection of confidentiality, integrity, availability of data, function and services of the medical device along with the specified product security context.
Security capabilities may be determined as suitable risk-control measures. The design and implementation of such capabilities need to comply with the state of the art (see Annex I, sections 17.2 (MDR) or 1, 4, 16.2 (IVDR)) and cover a wide range of technical areas.

Automatic Logoff
Audit Controls
Authorization
Configuration of Security Features
Cybersecurity Product Upgrades
Personal Data De-Identification
Data Backup and Disaster Recovery
Emergency Access
Personal Data Integrity and Authenticity
Malware Detection / Protection
Node Authentication
Person Authentication
Physical Locks
System and OS Hardening
Security and Privacy Guides
Personal Data Storage Confidentiality
Transmission Confidentiality
Transmission Integrity

Fonte: MDCG 2019-16, cit. - December 2019
(July 2020 rev. 1)

Cybersecurity & safety



Fonte: MDCG 2019-16, cit. - December 2019 (July 2020 rev. 1)

Cybersecurity+Safety per i DM

MDR - Regole di classificazione - Regola 11 - Allegato VIII

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.

Fonte: Bergamasco S.;
Le novità del Regolamento 2017/745 per l'ingegneria clinica. Centro Studi AIIC, 2021

MA

Sia nella MEDDEV 2.1/6 Qualification and Classification of stand alone software, sia nella MDCG 2019-11 Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 – IVDR è chiaramente specificato che qualora un software esegua una azione (su di un dato) e questa azione non sia "for the benefit of individual patients", allora il regolamento dispositivi medici non si applica

https://www.linkedin.com/pulse/lo-strano-caso-del-singolo-paziente-francesco-martelli/?trackingId=5wu6wDGZTb2k75uLpTy6Bg%3D%3D

Cybersecurity+Safety per i DM

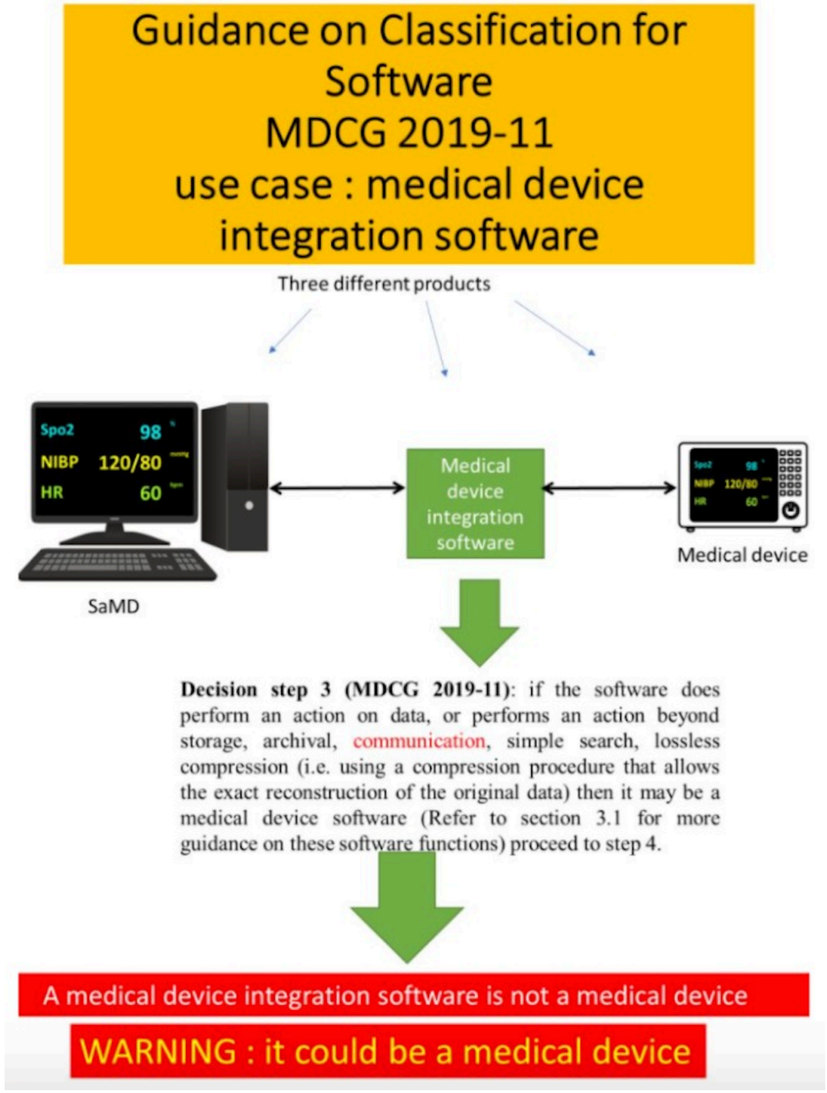
The qualification of #medicaldevice depends on the #intendeduse and it does not depend solely on technical / technological issues. It is wrong to qualify a device on technical /technological issues without taking into account its intended purpose. **If a manufacturer establishes an intended purpose within the definition of a medical device, this software is a medical device**. My opinion is that MDCG 2019-11 step 3 is in contrast to #MDR recital 19. In fact, **for the guideline if the software that performs only an action on the data, of "archiving, communication, simple search or lossless compression" is not a medical device regardless of the intended use**. This in my opinion is unacceptable and it does not comply with recital 19.

IEC 82304
4.5 System requirements

The MANUFACTURER shall specify and document the system requirements for the HEALTH SOFTWARE PRODUCT. These requirements shall include the functionality for INTENDED USE and, as applicable:

4.5 f)	features that allow for SECURITY compromises to be detected, recognized, logged, timed, and acted upon during normal use;
4.5 g)	features that protect essential functions, even when the software SECURITY has been compromised;

ESSENTIAL FUNCTION
function or capability that is required to maintain BASIC SAFETY, ESSENTIAL PERFORMANCE, a minimum of clinical functionality as specified by the manufacturer, and operational availability for the MEDICAL DEVICE

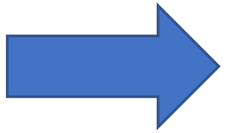


https://www.linkedin.com/in/antoniobartolozzi/detail/recent-activity/

Modello Cybersecurity+Privacy+Safety per i DM

L’analisi e la valutazione del rischio che consideri anche la safety del paziente, oltre alla privacy e alla cybersecurity e all’efficacia del DM, non può essere svolta solo dal produttore, ma deve essere in capo anche all’organizzazione responsabile:

- ❑ Safety del paziente e degli operatori/utilizzatori
- ❑ Distruzione, perdita, modifica, non disponibilità del dato
- ❑ Rilevazione di malware e vulnerabilità
- ❑ Condizioni ambientali e contesto (*mobile*, IoT, ecc…)
- ❑ Attuazione di controlli che non impattino sulla safety
- ❑ Mantenere elevati livelli di efficenza (effectiveness)



RISERVATEZZA
INTEGRITA’
DISPONIBILITA’
(RESILIENZA)
(RILEVABILITA’ DEL RISCHIO)

GDPR, NIS, AgID, Garante, CSIRT, Piano Nazionale Cybersicurezza…

L'obiettivo è garantire la **massima protezione dei dati sanitari e dei pazienti** promuovendo allo stesso tempo lo sviluppo di nuove tecnologie nella cura della persona

Identificare i principali rischi e adottare contromisure per mitigarli (ISO 31000)
Dare priorità agli interventi, in base alle risorse disponibili - utilizzare controlli e misure (ISO 27001)
Monitorare e mantenere un rischio residuo in un processo di possibile miglioramento continuo

Organizzazione Responsabile e Ambiente Operativo

D.Lgs. 81/08 –Art. 71 Obblighi del datore di lavoro

…

4. Il datore di lavoro prende le misure necessarie affinché:
   a) le attrezzature di lavoro siano:
   b) installate ed utilizzate in conformità alle istruzioni d'uso;
   c) oggetto di idonea manutenzione al fine di garantire nel tempo la permanenza dei requisiti di sicurezza di cui all'articolo 70 e siano corredate, ove necessario, da apposite istruzioni d'uso e libretto di manutenzione;

…

Le responsabilità in merito alle scelte manutentive (affidarsi al fabbricante? A ditte terze di global service? Avere un servizio in-house) restano in capo al «datore di lavoro» della struttura che utilizza i dispositivi

Fonte: Bergamasco S.; cit., 2021

Organizzazione Responsabile e Ambiente Operativo

ISO/IEC 80001
responsability agreement…

ISO 27701
estende il sistema di gestione della sicurezza delle informazioni (ISO 27001 e ISO 27002) per includere le particolarità del trattamento dei dati personali:

- determinare il ruolo dell'organizzazione ad essere certificata (titolare del trattamento, subappaltatore);
- gestione unificata dei rischi informatici per l'organizzazione e dei rischi per la privacy delle persone interessate;
- consapevolezza del personale, classificazione dei dati, protezione dei supporti rimovibili, gestione degli accessi e crittografia dei dati, backup dei dati, registrazione degli eventi;

Organizzazione Responsabile e Ambiente Operativo

MDCG 2019-16
ambiente operativo (requisiti IT per operatività e funzionamento DM nelle organizzazioni responsabili)

- compliance con il GDPR;
- attuazione controlli di sicurezza:
  - credenziali di accesso al DM,
  - policy di accesso per utenti e amministratori,
  - sistemi antivirus o antimalware,
  - firewall,
  - una lista delle applicazioni e dei software consentiti (misure minime Agid);
- sistemi di controllo e di sicurezza per il traffico e gli apparati di rete (NIS);
- se DM usato in combinazione con sistemi IT:
  - possibilità di hardening,
  - controllo accessi,
  - AV,
  - utilizzo controlli/misure che non pregiudichino destinazione d'uso, funzionalità, interoperabilità,
  - analisi rischi del produttore,…
- altre misure e controlli: patch management, partizionamento rete, autenticazione macchina, VA, ecc…

Parte 1.3

modelli, tecniche e tecnologie per la cybersecurity dei DM

Materiali e metodi - analisi e valutazione del rischio DM

Calcolo di un IVR (Indice di Valutazione del Rischio) per i DM che includesse aspetti di cybersicurezza, safety, efficacia collegati ad un contesto / mondo che cambia

Selezione di **32 DM pilota** collegati ad una rete IT-medicale e… a un mondo che cambia… (new normal)

Utilizzo di **quattro categorie** del rischio: **documentazione e manutenzione, safety (sicurezza del paziente), sicurezza IT e privacy, contesto**.

Viene correlata la valutazione di impatto per la **protezione dei dati** con le misure e i rischi riportati nel GDPR: accesso illegittimo / illecito, perdita di dati, modifica dei dati

Integrazione della categoria di rischio "**contesto**" che tiene conto del "mondo che cambia" e dell'uso/adozione di tecnologie che portano i DM verso l'esterno (*mobile computing*) o li collegano a risorse esterne (vedi cloud)

Utilizzo di **metodi statistici** (regressione lineare e metodo logistico) per ottenere una equazione dell'IVR (analisi del rischio)

Utilizzo di un controllo HW su un DM per valutare i risultati di una auspicabile **mitigazione del rischio** calcolando l'IVR pre-applicazione della misura/controllo e post applicazione

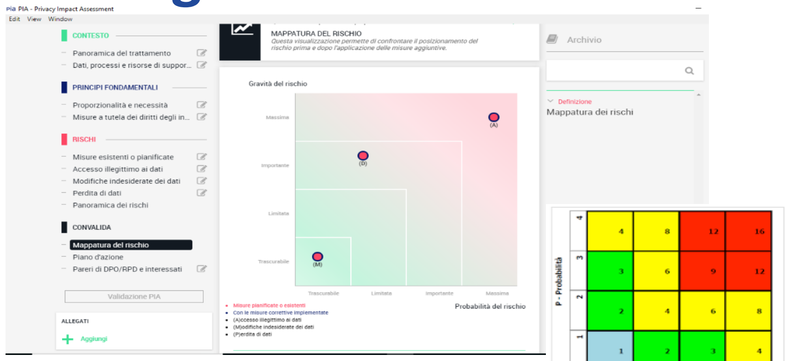
Materiali e metodi

Dispositivo	Modello
SPETTROMETRO DI MASSA	API 3200 QTrap
MODULO PER HPLC (PC)	Waters 717
SPETTROMETRO DI MASSA	API 3200 Q TRAP
SPETTROMETRO DI MASSA	5973 MSD
ELETTROENCEFALOGRAFO (eeg)	tor 500
EMG	BRAIN QUICK BQ3200
ELETTROCARDIOGRAFO (ecg)	eli250
ECOTOMOGRAFO	VIVID E 95
ECOTOMOGRAFO	PROSOUND ALPHA 10
ECOTOMOGRAFO PORTATILE	VIVID I
ENDOSCOPIO	ENDOX
AMPLIFICATORE DI SEQUENZE NUCLEOTIDICHE	MIC4 Channel
TAC	Philips
stampante di lastre	sij400
telecomandato	luminos drf max
ELETTROENCEFALOGRAFO	HEWLETT PACKARD CO
COAGULOMETRO (PC)	STA COMPACT
MONITOR ACQUISIZIONI IMMAGINI (sistema aida 27959)	20046120 AIDA CONTROL NEO
ECOGRAFO GE	VOLUSON E10
ECOGRAFO PROSOUND ALFA 7	PROSOUND ALPHA 7
ECOTOMOGRAFO VOLUSON E8	VOLUSON E8
ECOGRAFO GE	VOLUSON 730 EXPERT
ECOTOMOGRAFO	VOLUSON E10
TOMOGRAFO A RISONANZA MAGNETICA	INGENIA 1,5T
WORKSTATION DI REFERTAZIONE RMN (telemedicina)	DELL Optiplex
DIAGNOSI DELL'APPARATO DIGERENTE A CAPSULA DEGLUTTIBILE	DATA RECORDER 3
ELETTROENCEFALOGRAFO	BRAIN QUICK BQ3200 ACQ
ELETTROCARDIOGRAFO	ELI 350
ELETTROCARDIOGRAFO	ELI 350
EMOGASANALIZZATORE (collegato a rete ASUGI)	ABL 800
EMOGASANALIZZATORE	ABL 90 FLEX
IonTorrent	ION TORRENT SEQUENCER

I 32 DM

Studi precedenti: privacy + security

Materials and methods – REI risk factors and categories



PRIVACY-PIA			
(P1) DATA	(P2) ULAWFUL DATA ACCESS	(P3) DATA MODIFICATION	(P4) DATA LOSS
ANONYMIZATION/ ENCRYPTION=0	MAX=1	MAX=1	MAX=1
PERSONAL DATA= 0.5	IMPORTANT=0.66	IMPORTANT=0.66	IMPORTANT=0.66
SPECIAL PERSONAL DATA= 1	LIMITED=0.33	LIMITED=0.33	LIMITED=0.33
	NEGLIGIBLE=0	NEGLIGIBLE=0	NEGLIGIBLE=0

Studi precedenti: privacy + security

Materials and methods – statistical methods (weights calculation)

MULTIPLE LINEAR REGRESSION (MLR) MODEL/METHOD:

Meets the objective of studying the dependence of a quantitative variable Y (the REI) on a set of n quantitative explanatory variables X1, ..., Xn, called predictors (the risk factors), for each MD, using a linear model.

$$\mathbf{IVR} = \begin{pmatrix} A11 & \cdots & A1j \\ \vdots & \ddots & \vdots \\ Ai1 & \cdots & Aij \end{pmatrix} \begin{matrix} X1 \\ \vdots \\ Xj \end{matrix} + \begin{matrix} c1 \\ \vdots \\ cj \end{matrix} \quad \text{for i MD}$$

LOGISTIC MODEL/METHOD:

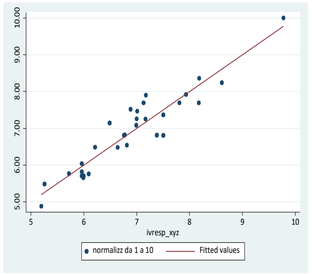
There are risk factors X1, ..., Xn measurable, and an output Y that is dichotomous: 0 or 1, while the predictors assume generic real values, as in traditional linear multiple regression.

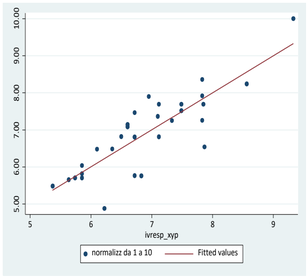
Studi precedenti: privacy + security

Results – MLR Model

IVR	0 BASSO-MEDIO	1 ALTO	TOTALE
5.197069	1	0	1
5.25547	1	0	1
5.72017	1	0	1
5.962609	3	0	3
5.993913	1	0	1
6.000978	1	0	1
6.09309	1	0	1
6.213079	1	0	1
6.486822	0	1	1
6.642969	1	0	1
6.759453	1	0	1
6.772733	1	0	1
6.816737	1	0	1
6.887031	0	1	1
6.994827	0	1	1
7.001647	0	1	1
7.009923	0	1	1
7.12947	0	1	1
7.167182	0	1	1
7.174247	0	1	1
7.37994	1	0	1
7.502832	1	1	2
7.80983	0	1	1
7.932722	0	1	1
8.176784	0	1	1
8.183192	0	1	1
8.613083	0	1	1
9.779943	0	1	1
TOTALE	16	15	31

Xi, Yi, Zi





P<0.1

$$IVR_{RLM1} = 1.267733 + 1.289753 * z_3 + 1.360721 * x_2 - 0.7590005 * x_3 + 1.01601 * z_1 + 3.436427 * y_4 + 0.4929089 * z_6 + 1.166861 * y_3$$

IVR	0 BASSO-MEDIO	1 ALTO	TOTALE
5.370118	1	0	1
5.636159	1	0	1
5.739188	1	0	1
5.853402	3	0	3
6.099929	1	0	1
6.222472	1	0	1
6.35133	1	0	1
6.49787	1	0	1
6.602726	0	2	2
6.7204	3	1	4
6.829741	1	0	1
6.952283	0	1	1
7.100654	0	1	1
7.113241	1	1	2
7.332537	0	1	1
7.487411	0	2	2
7.830465	0	3	3
7.848152	0	1	1
7.867665	1	0	1
8.560276	0	1	1
9.327287	0	1	1
TOTALE	16	15	31

Xi, Yi, Pi

P<0.05

$$IVR_{RLM2} = 4.517765 + 0.7670108 * y_3 + 1.459622 * x_2 + 1.464495 * p_2 + 1.118394 * p_4$$

With equal results (number of MDs correctly classified: 14 of 16 at low risk, 12 of 15 at high risk) and with a lower P (P <0.05), the equation with Pi is computationally more profitable and effective

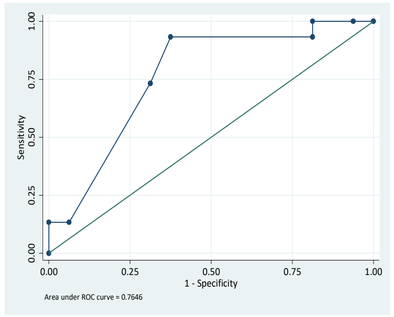
Studi precedenti: privacy + security

Results – logistic model

Using Zi (IT Security) and Pi (Privacy)

Xi, Yi,

Pr(ivresp)	0	1	Total
.0261295	1	0	1
.0538722	2	0	2
.1030915	0	1	1
.1179561	7	0	7
.5861655	1	3	4
.6894978	4	9	13
.7107756	1	0	1
.9592164	0	2	2
Total	16	15	31



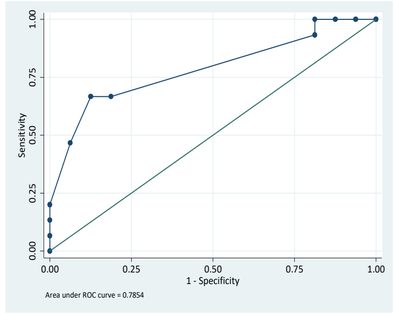
Sensitivity=93,33%
Specificity= 62,58%
Correctly classified=77,42%

P<0.15

$$IVR_{LOG1} = -11.04666 + 2.360065 * y_3 + 9.034736 * y_4 + 2.809702 * z_3$$

Xi, Yi,

Pr(ivresp)	0	1	Total
.0068564	1	0	1
.0332188	1	0	1
.1616833	1	0	1
.184903	0	1	1
.3181692	10	4	14
.5996258	1	0	1
.7237025	1	3	4
.7549489	1	4	5
.9453334	0	1	1
.9531385	0	1	1
.991317	0	1	1
Total	16	15	31



Sensitivity=66,67%
Specificity= 87,50%
Correctly classified=77,42%

P<0.15

$$IVR_{LOG2} = -11.19683 + 3.774763 * x_2 + 1.7251 * y_3 + 10.43464 * y_4$$

There are no significant differences in use of Zi or Pi

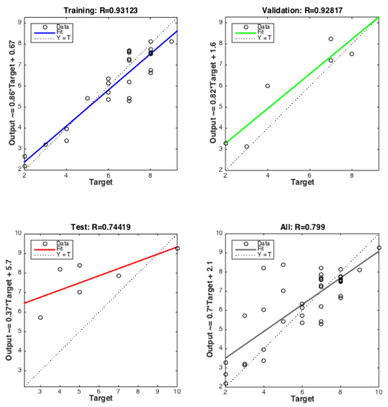
Studi precedenti: utilizzo di reti neurali

Neural Networks methods and results

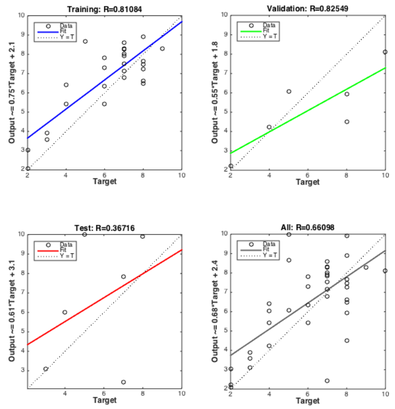
NEURAL NETWORK START - MATLAB

- Two layer feedforward network with, respectively, 10, 15 and 5 hidden neurons
- Supervised learning algorithm: Levemberg-Marquardt;
- Only three risk categories considered (not privacy)
- Not so brilliant results -> pilot study and reduced training and test set

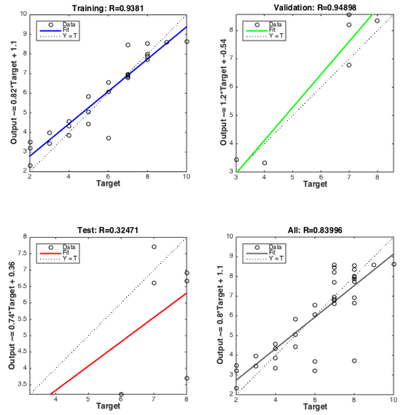
TRAINING SET : 27 of 39 MDs (the study was extended from 31 to 39 MD)
TEST SET: 6 of 39 MDs
VALIDATION SET: 6 of 39 MDs



- 7 of 10 MD at low risk;
- 12 of 18 MD at medium risk;
- 9 of 11 MD at high risk;



- 7 of 10 MD at low risk;
- 6 of 18 MD at medium risk;
- 6 of 11 MD at high risk;



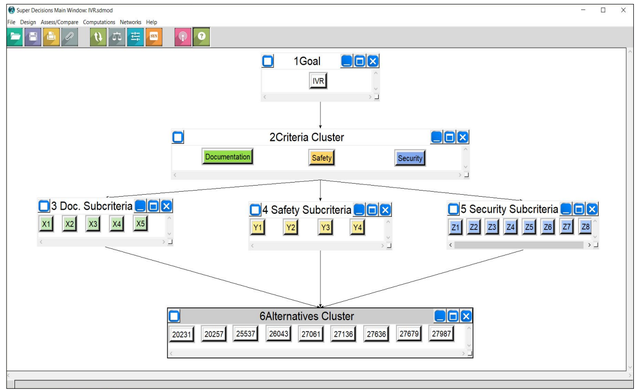
- 9 of 10 MD at low risk;
- 11 of 18 MD at medium risk;
- 8 of 11 MD at high risk;

Studi precedenti: utilizzo del metodo AHP

AHP method and results

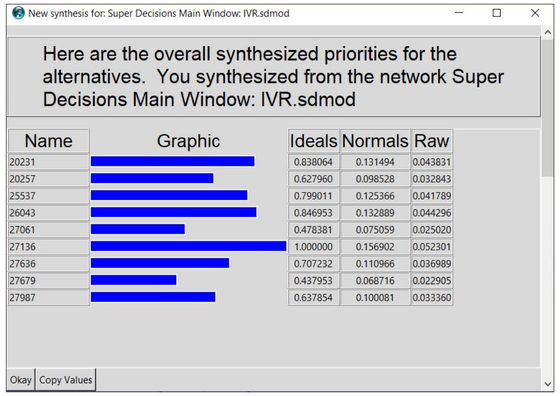
ANALYTIC HIERARCHY PROCESS

- Calculus of the REI of 9 selected MDs using the application of the multi-criteria and compensatory AHP method, considering both IT security and Privacy risk categories
- The method is used as a solution to decision problems in various sectors, helping the decision maker to obtain a compromise but robust solution
- The AHP method is provided by the use of a comparison between pairs of quantitative and ordinal elements for evaluation, and estimating the reciprocal matrix of each risk category and therefore the main eigenvector of the matrix



The AHP model and the risk categories

The obtained risk classification of the 9 MDs



Comparison with MLRM (with IT Security)

ETICHETTA	POSIZIONE $_{MRLM}$	POSIZIONE $_{AHP}$	
27136	1	1	=
26043	2	2	=
20257	3	7	-
27679	4	9	-
27636	5	5	=
20231	6	3	+
27061	7	8	-
25537	8	4	+
27987	9	6	+

Comparison with logistic method (with Privacy)

ETICHETTA	POSIZIONE $_{LOG}$	POSIZIONE $_{AHP}$	
27136	1	1	=
26043	2	2	=
27061	3	5	-
27987	4	4	=
27679	5	6	-
27636	6	3	+

«Only» 9 MD compared; computational expensive

Studi precedenti: tensori e matrici

Matrix method and early results

Kronecker matrix product

- DPIA & MDIA (Medical Device Impact Assessment -> incorrect or defective intended use of the MD; incorrect or defective mainteinance of the MD; incorrect or defective modification of the MD)
- Matrix product DPIA X MDIA -> no predictive but effective and immediate (visual) risk analysis
- Calculus of the single DPIA and MDIA risk matrix for 5 MDs and then, using the Kronecker product, creation of a matrix of order 16 (4x4) for each MD -> only the 9 "intersection points" are considered (1st order problem) -> visual map of the risk
- More correlations may be found -> cross-related & concurrent risks

D.M.	Fattori di rischio PIA			Fattori di rischio MDIA		
	Accesso illegittimo dati (A)	Modifica dati (M)	Perdita dati (P)	Destinazione d'uso diversa (U)	Scorretta manutenzione (S)	Modifica sistema EM (E)
1	1x3	2x3	1x2	2x1	2x1	2x2
2	1x1	1x1	1x1	1x3	1x3	2x3
3	2x3	1x1	1x1	1x1	1x4	2x4
4	2x3	1x1	1x1	1x1	1x3	2x2
5	1x1	1x1	2x4	1x1	4x1	2x2

K =

16	32	48	64	32	64	96	128	48	96	144	192	64	128	192	256
12	24	36	48	24	48	72	96	36	72	108	144	48	96	144	192
8	16	24	32	16	32	48	64	24	48	72	96	32	64	96	128
4	8	12	16	8	16	24	32	12	24	36	48	16	32	48	64
12	24	36	48	24	48	72	96	36	72	108	144	48	96	144	192
9	18	27	36	18	36	54	72	27	54	81	108	36	72	108	144
6	12	18	24	12	24	36	48	18	36	54	72	24	48	72	96
3	6	9	12	6	12	18	24	9	18	27	36	12	24	36	48
8	16	24	32	16	32	48	64	24	48	72	96	32	64	96	128
6	12	18	24	12	24	36	48	18	36	54	72	24	48	72	96
4	8	12	16	8	16	24	32	M/U M/S 12	24 M/E	36	48	16	32	48	64
2	4	6	8	4	8	12	16	6	12	18	24	8	16	24	32
4	8	12	16	8	16	24	32	12	24	36	48	16	32	48	64
3	6	9	12	6	12	18	24	9	18	27	36	12	24	36	48
2	4	6	8	P/U P/S 4	8 P/E	12	16	A/U A/S 6	12 A/E	18	24	8	16	24	32
1	2	3	4	2	4	6	8	3	6	9	12	4	8	12	16

«Only» 5 MD studied; early results in MDs risk evaluation similar to the REI obtained with MLR and AHP methods

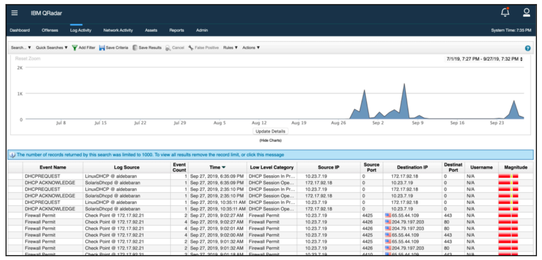
Studi precedenti: risultati preliminari utilizzo Controllo HW

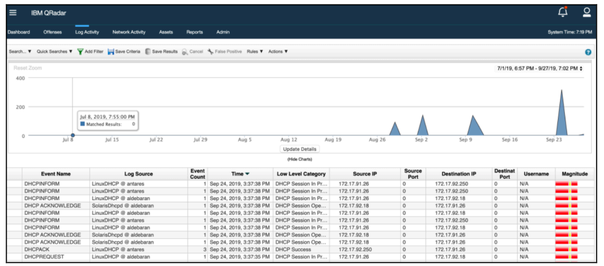
Early results using a HW Control for MD Cyber-Security

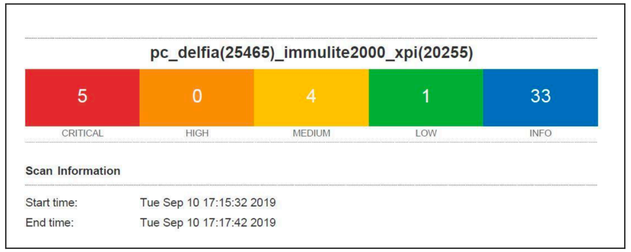
- Use of Nessus 7.1.1 Vulnerability Professional Scanner (Basic Network Scan) & Zenmap
- Traffic monitor analyzed with Qradar SIEM – IDS Sguill and Elsa/Wireshark protocol Analyzer (Kali Linux and Security Onion distribution)
- Use on MD that cannot be enforced with restrictive or controlled security policies

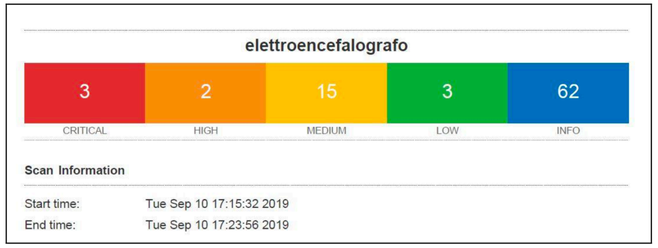
- Evaluation of Vulnerabilities pre and post the use of the device: two MD analyzed (pc Delfia – EEG)
- Preliminary results

Controllo HW









Materiali e metodi – modelli statistici per il calcolo dei pesi dell'IVR

$$IVR = aX + bY + cZ + \mathbf{dC}$$

X: DOCUMENTAZIONE E MANUTENZIONE

Y: RISCHIO PER IL PAZIENTE

Z: SICUREZZA INFORMATICA E PRIVACY

C: CONTESTO

a,b,c,d: pesi da valutare

MODELLO / METODO DI REGRESSIONE LINEARE MULTIPLA (RLM):

Soddisfa l'obiettivo di studiare la dipendenza di una variabile quantitativa Y (l'IVR) da un insieme di n variabili esplicative quantitative X1, ..., Xn, chiamate predittori (i fattori di rischio), per ogni DM, utilizzando un modello lineare.

$$\mathbf{IVR} = \begin{pmatrix} A11 & \cdots & A1j \\ \vdots & \ddots & \vdots \\ Ai1 & \cdots & Aij \end{pmatrix} \begin{matrix} X1 \\ \vdots \\ Xj \end{matrix} + \begin{matrix} c1 \\ \vdots \\ cj \end{matrix} \quad \text{for i DM}$$

MODELLO / METODO OGISTICO:

Esistono fattori di rischio X1, ..., Xn misurabili e un output Y dicotomico: 0 o 1, mentre i predittori assumono valori reali generici, come nella tradizionale regressione lineare multipla.

Materiali e metodi – Le categorie e i fattori di rischio

DOCUMENTAZIONE E MANUTENZIONE			
(X1) DOCUMENTAZIONE	**(X2) COSTO DI MANUTENZIONE**	**(X3) MANUTENZIONE PREVENTIVA**	**(X4) MANUTENZIONE CORRETTIVA 2018-2020**
COMPLETA (CON MAN. IN ITALIANO)=0	GLOBAL SERVICE/ GARANZIA=0	MP EFFETTUATA DA MENO DI UN ANNO/ GARANZIA=0	NESSUNA=0
COMPLETA (CON MAN. D'USO IN INGLESE)= 0.5	CONTRATTO=0.5	MP EFFETTUATA DA Più DI UN ANNO / SERVICE/ DOC. INCOMPLETA O NON REPERIBILE=0.5	DA 1 A 3=0.33
NON COMPLETO/NON REPERIBILE=1	SENZA CONTRATTO=1	2 INTERVENTI DI MP NON EFFETTUATI=1	DA 4 A 8= 0.66
	DOCUMENTAZIONE ASSENTE=1	DOCUMENTAZIONE ASSENTE= 1	Più DI 8 (O DOCUMENTAZIONE ASSENTE) = 1

Materiali e metodi – Le categorie e i fattori di rischio

RISCHIO PER IL PAZIENTE			
(Y1) TIPOLOGIA APPARECCHIATURA	**(Y2) CONSEGUENZE PER IL PAZIENTE IN CASO DI GUASTO**	**(Y3) ETA' dell'APPARECCHIATURA (anni)**	**(Y4) FREQUENZA DI UTILIZZO**
TERAPEUTICA=1	MORTE=1	MAGGIORE O UGUALE A 8=1	UTILIZZO GIORNALIERO=1
DIAGNOSTICA=0.66	DANNO=0.75	MINORE DI 8 =0	ALMENO UN UTILIZZO ALLA SETTIMANA=0.75
ANALISI=0.33	TERAPIA INAPPROPRIATA=0.5		ALMENO UN UTILIZZO AL MESE=0.5
ALTRO=0	NESSUN RISCHIO SIGNIFICATIVO=0.25		ALMENO UN UTILIZZO ALL'ANNO=0.25

Materiali e metodi – Le categorie e i fattori di rischio

SICUREZZA INFORMATICA E PRIVACY						
(Z1) CREDENZIALI DI ACCESSO AL SISTEMA	**(Z2) ANTIVIRUS/ SOLUZIONI ZERO TRUST**	**(Z3) BACKUP/UPS**	**(Z4) VULNERABILITY ASSESSMENT**	**(Z5) FIREWALL/IPS/ SIEM**	**(Z6) PRIVACY - DPIA TRATTAMENTO**	**(Z7) SISTEMA OPERATIVO**
WHAT YOU ARE -HAVE = 0	ATTIVO E AGGIORNATO (CON ZERO TRUST)=0	GIORNALIERO/ UPS SI=0	CRITICITA' ASSENTI=0	ATTIVO + SCANSIONE SIEM NEGATIVA=0	NO PERDITA, ACCESSO, MODIFICHE DATI= 0	AGGIORNATO E PATCHATO=0
WHAT YOU KNOW / PASSWORD FORTE= 0,25	ATTIVO E AGGIORNATO (SENZA ZERO TRUST)=0,25	GIORNALIERO/ UPS NO O SETT/ UPS SI=0.25	1-2 CRITICITA'=0.33	ATTIVO + SCANSIONE SIEM POSITIVA=0,33	MAX ALMENO UNA DELLE TRE = 0,33	NON PATCHATO=0,33
CREDENZIALI DEBOLI=0.5	INSTALLATO E NON AGGIORNATO (NO ZT)=0.50	MENSILE/ CON-SENZA UPS=0.66	>2 CRITICITA'=0.66	NON ATTIVO + SCANSIONE SIEM NEGATIVA=0,66	MAX ALMENO DUE DELLE TRE = 0,66	NON AGGIORNATO=0,66
NON PRESENTI=1	NON PRESENTE MA INSTALLABILE (NO ZT)= 0.66	ANNUALE / CON-SENZA UPS= 0.75	>2 CRITICITA' + ALTTE VULNERABILITA' =0.75	NON ATTIVO + SCANSIONE SIEM POSITIVA=1	SI PERDITA, ACCESSO, MODIFICHE DATI / NO DPIA = 1	OBSOLETO=1
	NON RESENTI NON INSTALLABILI=1	NESSUN BACKUP /CON-SENZA UPS= 1	ELEVATA/NON EFFETTUATA=1			

Materiali e metodi – Le categorie e i fattori di rischio

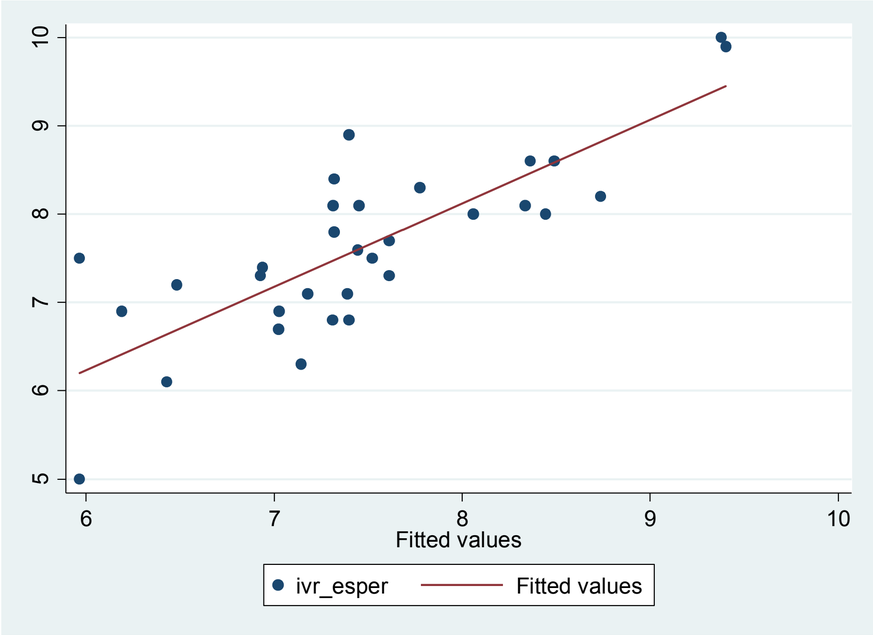
CONTESTO (CONDIZIONI AMBIENTALI)						
(C1) TIPOLOGIA DEL DATO	**(C2) PERIMETRO AZIENDALE (UTILIZZO)**	**(C3) USO IN/PER TELEMEDICINA**	**(C4) MOBILE**	**(C5) ALTRI RISCHI (CLINICO,ELETTRICO, EM…)**	**(C6) CLOUD/IoT**	**(C7) CRITTOGRAFIA DEI DATI/ BLOCKCHAIN**
DATO COMUNE= 0	USO NEL PERIMETRO=0	NO=0	ASSENTE=0	NO=0	NO=0	PUNTO PUNTO E ALTRE FORME=0
DATO PERSONALE=0.33	VPN=0.33	SI CON SW DM O DM=0.5	WI-FI=0.33	SI (almeno 1)=0.5	Hybrid=0.5	SOLO PUNTO PUNTO O CRITTOGRAFIA DEL DATO=0.5
DATO SENSIBILE=0.66	FUORI DAL PERIMETRO= 0.66	SI CON SW GENERICO =1	MOBILE=0.66	SI (almeno >3)=1	SI=1	NO=1
DATO ULTRA SENSIBILE=1	FUORI DAL PERIMETRO DISP NO AZIENDALE=1		WI-FI e MOBILE=1			

Risultati – Regressione lineare multipla

P<0.05 $IVR_{RLM} = 4.885831 + 0.7508848*x2 + 1.04312*y3 + 0.8905431*z4 + 1.249948*z5 + 0.8873042*z6 + 1.541112*c2$

IVR	BASSO	MEDIO	ALTO	TOTALE
5.9662221	1	1	0	2
6.188858	1	0	0	1
6.42859	1	0	0	1
6.481668	1	0	0	1
6.927285	1	0	0	1
6.938226	1	0	0	1
7.023084	1	0	0	1
7.026323	1	0	0	1
7.145525	1	0	0	1
7.179129	1	0	0	1
7.309159	1	0	0	1
7.313668	0	0	1	1
7.319133	0	1	1	2
7.389307	1	0	0	1
7.398526	1	0	1	2
7.446793	0	1	0	1
7.451604	0	0	1	1
7.522618	0	1	0	1
7.610842	1	0	0	1
7.611943	0	1	0	1
7.773969	0	0	1	1
8.059469	0	1	0	1
8.336267	0	0	1	1
8.362253	0	0	1	1
8.444885	0	1	0	1
8.488844	0	0	1	1
8.737696	0	0	1	1
9.379388	0	0	1	1
9.404847	0	0	1	1
TOTALE	14	7	11	32

(>= 7.309..)	100.00%	57.89%	75.00%	2.3750	0.0000
(>= 7.313..)	100.00%	63.16%	78.12%	2.7143	0.0000
(>= 7.319..)	92.31%	63.16%	75.00%	2.5055	0.1218
(>= 7.389..)	84.62%	68.42%	75.00%	2.6795	0.2249
(>= 7.398..)	84.62%	73.68%	78.13%	3.2154	0.2088
(>= 7.446..)	76.92%	78.95%	78.12%	3.6538	0.2923
(>= 7.451..)	76.92%	84.21%	81.25%	4.8718	0.2740
(>= 7.522..)	69.23%	84.21%	78.13%	4.3846	0.3654
(>= 7.610..)	69.23%	89.47%	81.25%	6.5769	0.3439
(>= 7.611..)	69.23%	94.74%	84.38%	13.1539	0.3248
(>= 7.773..)	69.23%	100.00%	87.50%		0.3077
(>= 8.059..)	61.54%	100.00%	84.38%		0.3846
(>= 8.336..)	53.85%	100.00%	81.25%		0.4615



IVR	BASSO/MEDIO	ALTO	TOTALE
5.9662221	2	0	2
6.188858	1	0	1
6.42859	1	0	1
6.481668	1	0	1
6.927285	1	0	1
6.938226	1	0	1
7.023084	1	0	1
7.026323	1	0	1
7.145525	1	0	1
7.179129	1	0	1
7.309159	1	0	1
7.313668	0	1	1
7.319133	1	1	2
7.389307	1	0	1
7.398526	1	1	2
7.446793	1	0	1
7.451604	0	1	1
7.522618	1	0	1
7.610842	1	0	1
7.611943	1	0	1
7.773969	0	1	1
8.059469	1	0	1
8.336267	0	1	1
8.362253	0	1	1
8.444885	1	0	1
8.488844	0	1	1
8.737696	0	1	1
9.379388	0	1	1
9.404847	0	1	1
TOTALE	21	11	32

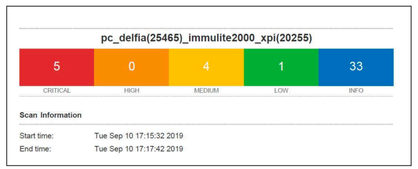
Assegnando rischio basso: 1-7.49; rischio medio: 7.5-8; rischio alto: 8.1-10 il modello identifica correttamente 13 su 14 DM a basso rischio

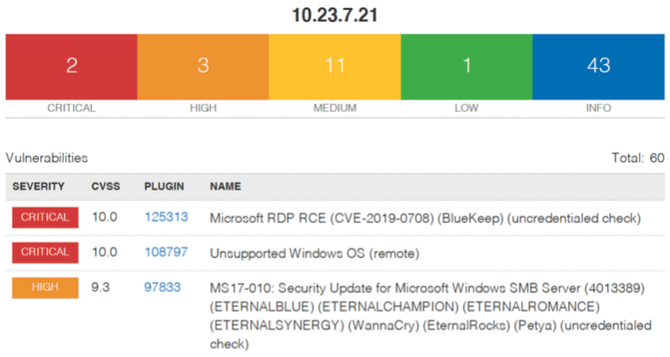
Se si scegliesse 1-7.309 come basso-medio rischio e 7.313-10 come alto rischio la predittività del modello migliora per l'alto rischio e il modello sovrastima il rischio per i DM a basso-medio rischio (abbiamo 7 falsi positivi): 11 su 11 ad alto rischio identificati

Risultati - Mitigazione del rischio

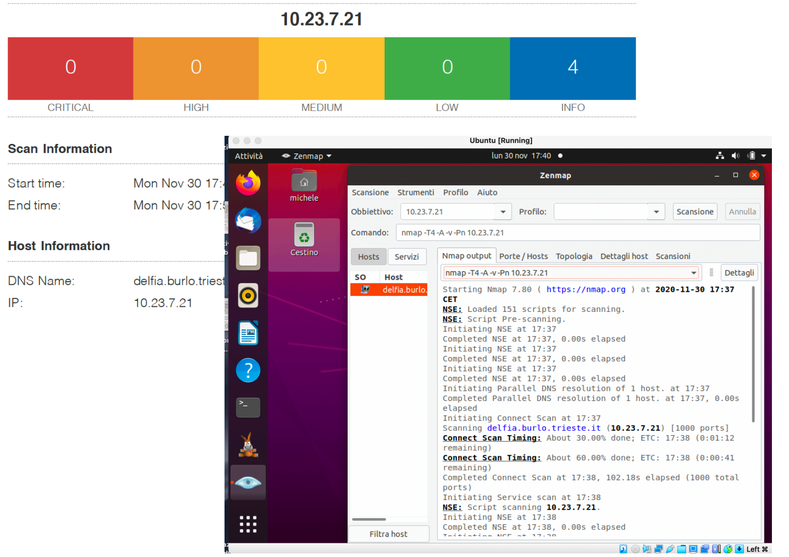
Un Controllo HW sulle porte e sul traffico è stato utilizzato prima e dopo il calcolo dell'IVR per un MD su cui era stato rilevato traffico anomalo e possibile compromissione dei dati

Dai valori ottenuto secondo il modello di regressione lineare (sia dicotomico che a tre stadi) il DM passa da una situazione ad alto rischio a una rispettivamente a basso-medio per il modello dicotomico (con cutoff a 7.773 e ROC a 91.5% e 87.5% DM correttamente classificati) e a basso rischio per il modello alto/medio/basso (cutoff a 7.45 e 81.5% DM correttamente classificati).





Controllo HW



Fattore	Valore	Valutazione
X2=	0.5	sistema sotto contratto con ditta esterna
Y3=	1	macchina in uso da più di 8 anni
Z4=	0.75	criticità elevate >2 e altre vulnerabilità rilevate
Z5=	1	firewall non attivo e scansione SIEM positiva
Z6=	0.66	DPIA con rischio MASSIMO per perdita e accesso indesiderato dati
C2=	0.33	macchina nel perimetro aziendale con accesso VPN

IVR_{delfia}= 9.316436457

IVR_{delfia}= 7.399649969

Fattore	Valore	Valutazione
X2'=	0.5	sistema sotto contratto con ditta esterna
Y3'=	1	macchina in uso da più di 8 anni
Z4'=	0.33	<1-2 criticità elevate rilevate
Z5'=	0	firewall attivo e scansione SIEM negativa
Z6'=	0.33	DPIA con rischio MASSIMO solo per perdita dati
C2'=	0.33	macchina nel perimetro aziendale con accesso VPN

Risultati - discussione

I modelli statistici ci hanno permesso di ottenere valori per l'IVR con una **buona specificità e sensibilità**, il che significa che la formula ottenuta è un buon modello predittivo per la valutazione dei rischi per i DM in uno scenario complesso come un Ospedale, che abbiamo detto, essere "in uscita" nel contesto attuale

Non sono stati rilevate delle co-linearità tra le categorie del rischio come in precedenti utilizzi del modello. Le nuove categorie invece sembrano aver aggiunto una nuova dimensione della realtà che viene indagata che si aggiunge alle precedenti dimensioni, arrivando a definire, visti i risultati ottenuti, una **buona descrizione di uno scenario complesso** e in continuo divenire.

Questi risultati confermano l'accuratezza e la ripetibilità del modello utilizzato con i metodi statistici, aprendo nuove possibilità nello studio e nella ricerca di **modelli integrati complessi e dinamici** (ML & AI) per l'analisi, la valutazione e la mitigazione del rischio

I risultati preliminari ottenuti utilizzando un Controllo HW **per la mitigazione del rischio** una volta calcolato l'IVR sono incoraggianti

Vedremo che risultati simili, **se non addirittura più incoraggianti**, sono stati raggiunti anche con altri device come l'EDGE IPS di TXOne-TrendMicro

Tali modelli vanno **integrati e inclusi** con soluzioni automatiche come Medigate dove sia possibile **inserire e misurare i fattori e le categorie di rischio** per ogni singolo DM e per tutti i DM appartenenti ad una Azienda Sanitaria.

Conclusioni (1)

La valutazione dei rischi che includa cybersecurity, reti IT e *mobile*, cloud, IoT, safety di pazienti e operatori e DM è un **problema multidimensionale** che implica, come abbiamo visto, una forte correlazione tra diverse grandezze rilevabili e stimabili che sono state identificate con i fattori e le categorie del rischio

Strumenti multi-ordine e multidimensionali possono essere utili per la valutazione del rischio (come l'integrazione dell'analisi DPIA nell'IVR o l'uso di misure/controlli di cybersicurezza) al fine di implementare un'analisi predittiva (o anche prescrittiva) sui DM, potendo tracciare, **monitorare e aumentare la sicurezza di dati ed informazioni che transitano sul singolo DM**

Un mondo che cambia è un mondo ***Anytime, Anywhere, Anyone, Any-device***. Il paradigma è quello dell'IoT ovvero l'*ubiquitous computing*

M-Health, IoHT, edge e cloud computing, Big Data e tutti i problemi e le preoccupazioni in materia di sicurezza informatica impongono ai produttori (MDR) e alle organizzazioni responsabili (Aziende Sanitarie) l'adozione di procedure, metodi, contromisure efficaci e affidabili e strumenti dinamici per **correlare gli eventi e fenomeni** di un mondo complesso.

L'E-Health non può fare a meno sia di **DM che escono dagli ospedali** e raggiungono il territorio e i device degli utenti, sia di un continuo monitoraggio di questi sistemi, della loro efficacia, sicurezza e safety

I DM come la privacy del dato (anzi a maggior ragione la privacy del dato nei DM) sono la cerniera tecnologica che avvicina e include le problematiche della cybersicurezza all'interno di una **sanità smart** (si potrà mai riuscire a superare l'ossimoro che sembra indicare la parola smart-health?) che per procedere ha bisogno di tecnologie biomediche sicure (safety+security) ed efficaci.

Conclusioni (2)

Parliamo da anni di **convergenza IC-IT**: a mio avviso il problema riguarda solo stabilire i reciproci domini di competenza e attuare tutti i possibili canali di **collaborazione e reciproco supporto** perché oggi il funzionamento dei DM non può prescindere da una accurata valutazione e gestione della sicurezza.

Come vedremo strumenti e piattaforme come Medigate consentono -con eventuali integrazioni con gestionali IT e IC e, nel caso specifico penso ad AITB- a tutti gli attori di vedere **le parti di loro pertinenza e interesse** prendendo atto della situazione di ciascuno. L'IT vede la **complessità e la delicatezza** del mondo medicale e l'IC **prende atto del e collabora al** continuo lavoro di analisi, rilevazione, pianificazione e mitigazione del rischio

Anche dinanzi ad un fornitore (quale che sia) oggi **non si può pensare di parlare con diverse voci**: IC e IT per quanto possibile stanno dalla stessa parte e questo aumenta il potere negoziale fin dalle prime fasi dell'acquisto di una tecnologia

L'IT **deve facilitare e sorveglia** tutte le operazioni relative al buon funzionamento del DM. Il raggiungimento di maggiore efficacia ed efficienza del DM è un risultato **vincente per entrambi**

Ritengo fondamentale in un mondo complesso come quello della security il **coinvolgimento** di esterni, di servizi, soluzioni, sistemi, know-how. Devono essere sempre più in atto forme di **partnership** che evidenzino competenze multiple e complementari.

La logica da adottare è win-win: **tutti vincono** se il DM è operativo al massimo delle sue funzionalità ed è sicuro. Questo riguarda l'approccio con le direzioni come la percezione dei colleghi e del pubblico

Se la security è un problema intrinsecamente dell'IT la safety e la privacy riguardano entrambi i servizi/strutture/uffici. **Sono argomenti trasversali** a tutto forse con un leggero sbilanciamento della safety verso l'IC. Ma abbiamo visto che safety e cybersecurity possono intersecarsi pericolosamente e quindi **l'approccio rimane comune**.

Grazie per l’attenzione

L’unica costante è il cambiamento
Buddha / Eraclito

Tutta la vita è risolvere problemi
K. Popper