La sicurezza informatica dei dispositivi medici collegati ad una rete ospedaliera

Ing. Michele Bava PhD
PO Informatica, Telefonia e DPO
Ufficio Sistema Informativo
SC Ingegneria Clinica, Informatica e Approvvigionamenti
IRCCS materno-infantile «Burlo Garofolo»

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

Description – Introduction

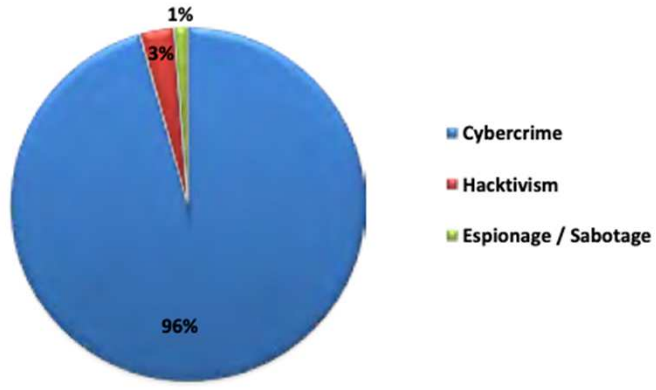
The connection of the MDs to an IT-medical network represents an advantage in patient's care but implies an accurate risk assessment, since the information exchanged is suitable to reveal the health status of the patient itself. The GDPR introduces the data protection impact assessment (DPIA) of processing into a new **security+privacy management model**, with the aim of managing and monitoring the risks associated with clinical and health data.

The purpose of this study is to propose an integrated numerical value of an index, the Risk Assessment Index (REI-IVR) calculated on the single MD (standalone, SW MDs, and/or SW used in combination with MD), considering the safe and effective use of the devices, the privacy and IT security of data and systems and, eventually, more risk factors and categories.

Description – Scenario (Rapporto CLUSIT 2019)

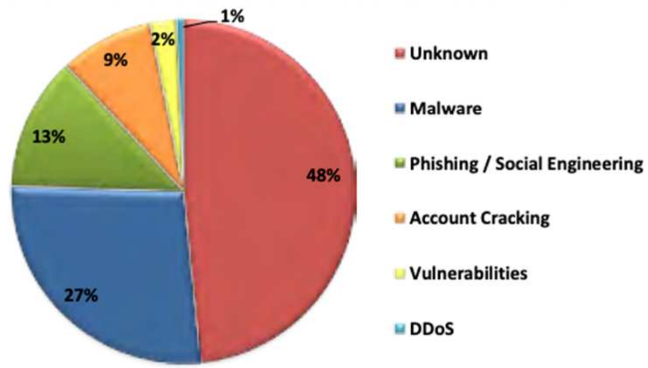
VITTIME PER TIPOLOGIA	2014	2015	2016	2017	2018	2018 su 2017	Trend
Gov - Mil - LEAs – Intel	213	223	220	179	252	40,8%	↗
Multiple targets	-	-	49	222	304	36,9%	↗
Health	32	36	73	80	159	98,8%	↑
Banking / Finance	50	64	105	117	156	33,3%	↗
Online Services / Cloud	103	187	179	95	129	35,8%	↗
Research – Education	54	82	55	71	110	54,9%	↑
Software / Hardware Vendor	44	55	56	68	109	60,3%	↑
Entertainment / News	77	138	131	115	102	-11,3%	↘
Critical Infrastructures	13	33	38	40	57	42,5%	↗
Hospitability	-	39	33	34	45	32,4%	↗
GDO / Retail	20	17	29	24	39	62,5%	↑
Others	172	51	38	40	30	-25,0%	↘
Org / ONG	47	46	13	8	18	125,0%	↑
Gov. Contractors / Consulting	13	8	7	6	14	133,3%	↑
Telco	18	18	14	13	11	-15,4%	↘
Automotive	3	5	4	4	9	125,0%	↑
Security Industry	2	3	0	11	4	-63,6%	↓
Religion	7	5	6	0	3	-	↗
Chemical / Medical	5	2	0	0	1	-	↗
TOTALE / MEDIA VARIAZIONI	873	1012	1050	1127	1552		

Tipologia e distribuzione degli attaccanti vs Healthcare - 2018



© Clusit - Rapporto 2019 sulla Sicurezza ICT in Italia

Tipologia e distribuzione delle tecniche d'attacco Healthcare - 2018



© Clusit - Rapporto 2019 sulla Sicurezza ICT in Italia

Description – Project Goals

- Unification of procedures and methods for assessing the risks of MDs that include, in addition to the regulatory framework of the MDs themselves, also IT security (AgID & Cybersecurity Act) and privacy according to the GDPR
- Risk evaluation of MD connected to Medical IT-Networks using different methods such as Multiple Linear Regression, Logistic Method, AHP, Neural Networks, Matrices
  - Assessing the weights of a formula or of a linear combination of vectors for the evaluation, the prediction and the mitigation of risks
- Creation of tools (i.e. a questionnaire) that objectively and repeatably correlates the data coming from the impact assessments of the processing (in the MD, in the SW MD and / or in the SW within the MD)
- Use of cybersecurity tools and devices (Vulnerability scanners, SIEM, IoT Defender) to reduce and mitigate the information security risk using MDs

Description – Project Goals and final users benefits

- Stakeholders:
  - CEOs and general managers <-> accountability, risk control and risk mitigation
  - Hospital risk managers and clinical engineers, IT managers involved in monitoring and managing of risk evaluation processes, which can measure risk and objectively assess the impact of the measures or controls they implement to mitigate it
  - Public and private agencies, companies or organizations, automated monitoring services that can keep track over time of analysis and actions taken, thanks to an integrated risk management approach which considers different and complementary aspects
  - Patients…

REGIONE AUTONOMA FRIULI VENEZIA GIULIA
istituto di ricovero e cura a carattere scientifico
Burlo Garofolo di Trieste
BURLO

Description – Technical standards and regulatory

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

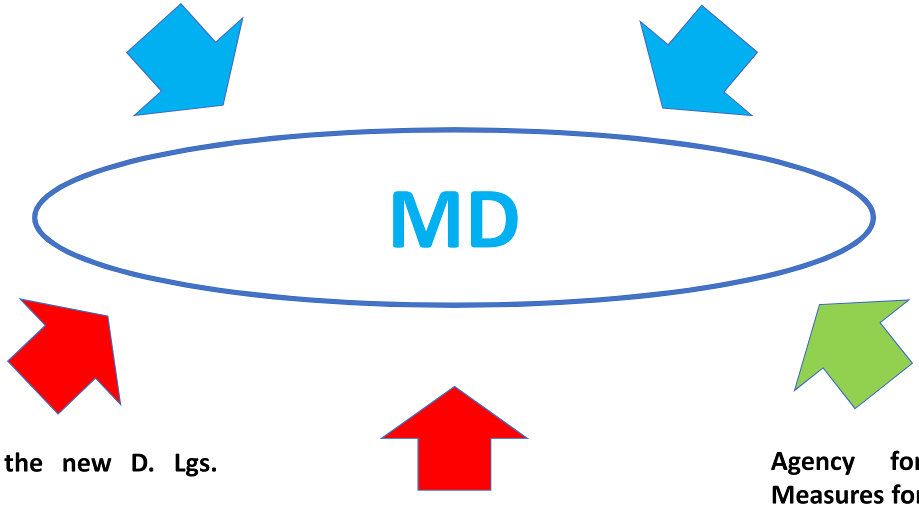
UNI ISO 31000: RISK MANAGEMENT

ISO IEC 27001: INFORMATION SECURITY MANAGEMENT SYSTEMS; NIST Cybersecurity Framework; National Cybersecurity Framework; CSC Model

Description – EU Regulation and National Laws

93/42/CEE AND 2007/47/CE DIRECTIVES & EU 2017/745 MEDICAL DEVICE REGULATION (May 2020)

MEDDEV 2.X/Y Guidelines with 1<X<12 e 1<Y<4 (including the revisions)



Italian D.Lgs 196/2003 and the new D. Lgs. 101/2018

GDPR – EU 2016/679 REGULATION, EU 881/2019 CYBERSECURITY ACT (2021) and European Directive 2016/1148

Agency for Digital Italy: Minumum Measures for the Public Administration (PA) security – National Plan for Information Security in the PA; Italian Data protection Authority

Description – Misure minime di sicurezza ICT per le PA

- Fanno riferimento al modello CSC (Critical Security Controls) predisposto da Sans Institute nel 2015 che riporta 20 classi di controllo ordinate per efficacia, divise in 3 famiglie (System, Network, Application) e divisi in 2 sub controlli (Foundational e Advanced)
- AgID ha introdotto un terzo sub controllo (Minimo, Standard, Alto) e ha selezionato 8/20 classi chiamandole ABSC (AgID Base Security Control).
- Top 5 dalla Sans 20 v6, le altre 3 dalla v5.

ABSC1: inventario dei dispositivi autorizzati e non autorizzati
ABSC2: inventario dei sw autorizzati e non autorizzati
ABSC3: protezione di configurazioni hw e sw sui dispositivi mobili, laptop, ws e server
ABSC4: valutazione e correzione continua della vulnerabilità
ABSC5: uso appropriato dei privilegi di amministratore
ABSC8: difese contro i malware
ABSC10: copie di sicurezza
ABSC13: protezione dei dati

Description – Regulation EU 2016/679 - GDPR

Fundamental principles:

- ❑ Safeguard the rights and freedoms of the data subject, the data subject's human dignity and legitimate interests and fundamental rights
- ❑ Accountability: responsibility of the controller (and processors) (Art. 24)
- ❑ Lawfulness, fairness and transparency; data minimization (relevant and limited) and accuracy
- ❑ Security of the personal data (CIA Triad)
- ❑ Privacy Impact Analysis and risk analysis and management (Art. 35)
- ❑ Focus on the DATA
- ❑ Appropriate technical and organizational measures (Art. 32)
- ❑ Record of processing activities e the DPO (Artt. 30 e 37)

In healthcare -> integrated model of security + privacy risk management

Description – Privacy + Security

Privacy and security risk evaluation in healthcare:
The GDPR provides for the data controller to construct a risk map that allows an estimate of the generic risk index for each type of processing.

- ❑ DPIA (Data Protection Impact Assessment) and PIA (privacy impact assessment)

- ❑ Information Security Risk Analysis Models (qualitative or quantitative)

- ❑ Risk value chain:
  - ❑Determination of threats; assessment of vulnerabilities (infrastructure, logical, services, organizational) and possible exploits
  - ❑Risk analysis -> evaluation of initial risk
    - ❑Evaluation of possible material/physical damages/probabilities
    - ❑Evaluation of possible immaterial (subjects' rights an fundamental violation, logical) damages/probabilities
  - ❑Applicable controls and measures (technical or organizational) to mitigate the initial risk
  - ❑Evaluation of residual risk -> (PDCA)

REGIONE AUTONOMA FRIULI VENEZIA GIULIA
Istituto di ricovero e cura a carattere scientifico
Burlo Garofolo di Trieste

cybersecurity act incoming…

Description – Privacy & Security

Cybersecurity Act – EU 881/2019

Strengthen the resilience to cyber attacks and create a single market of cyber security in terms of products, services and processes, increasing consumer confidence in digital technologies (the birth of a EC cybersecurity mark?)

The role of ENISA (European Union Agency for Cybersecurity

Description – Privacy & Security

Risk assessment and evaluation:

Risks involved in personal data processing:

Privacy

- ❑ Data destruction or not availability
- ❑ Data loss
- ❑ Data modification
- ❑ Unauthorized data diffusion and disclosure
- ❑ Accidental or unlawful access to data

Security

CONFIDENTIALITY

INTEGRITY

AVAILABILITY

(Resilience of systems and services)?

The objective is to ensure the maximum protection of patients' health data while promoting the development of new technologies in personal care

- ❑ Identify the major risks and take countermeasures to mitigate them
- ❑ Give priority to interventions, based on available resources
- ❑ Evaluate and maintain a residual risk

Materials and methods

The study was carried out mainly at the ICT Office of the IRCSS "Burlo Garofolo" of Trieste

For the impact assessment a questionnaire has been developed and re-elaborated which re-proposes* the CNIL's (French Data Protection Authority) PIA software. The questionnaire was applied to 30 Medical Devices for which the degree of protection was obtained for unlawful access, modification and loss of data.

The degree of protection was used to calculate the likelihood/probability and severity of risk necessary for calculating the classical risk matrix. These values were then reported as factors and risk categories within the REI, providing input to the statistical, neural and matrix models that allowed us to obtain the weights for calculating the REI for each DM.

*The Authority's PIA tool immediately has been evaluated too generic for assessing impact in Healthcare and does not objectively correlate the output data (risk matrix) with the evaluation that is carried out regarding data loss, data modification, illegitimate access

REGIONE AUTONOMA FRIULI VENEZIA GIULIA
istituto di ricovero e cura a carattere scientifico
Burlo Garofolo di Trieste
BURLO

Materials and methods

REI calculated for the MDs

Selection of 40 pilot MDs connected to the IT-medical networks

Creation of a questionnaire which correlates the impact assessment with the planned measures and risks in the three sections of the Authority’s PIA: illegitimate/unlawful access, loss of data, modification of data

Integration of the risk category of «Privacy» with those already present and reformulation of the REI model (privacy and IT security integrated model) for the MDs selected

Use of the IoT Defender to evaluate the results of a Vulnerability Assessment (pre and post)

Use of statistical methods, matrix methods, analytical hierarchy process method and neural networks methods to obtain the REI or a map of the risk

Materials and methods

The 40 MDs

1	AMPLIFICATORE DI SEQUENZE NUCLEOTIDICHE	15	DIAGNOSI DELL'APP. DIGERENTE A CAPSULA DEGLUTTIBILE	29	ANALIZZATORE AUTOMATICO PER IMMUNOCHIMICA (PC)
2	SISTEMA AUDIOMETRIA (PC)	16	SOFTWARE MEDICALE PER DIAGNOSI APP. DIGERENTE	30	PC CON GESTIONALE AL QUALE SONO COLLEGATI (28) E (29)
3	ELETTROENCEFALOGRAFO (1)	17	ELETTROENCEFALOGRAFO (2)	31	ANALIZZATORE AUTOMATICO PER IMMUNOCHIMICA (PC)
4	SISTEMA DI RADIOLOGIA DIGITALE (PC)	18	ELETTROENCEFALOGRAFO (3)	32	ANALIZZATORE AUTOMATICO PER IMMUNOCHIMICA (PC)
5	SISTEMA PER FLUOROANGIOGRAFIA (PC)	19	ELETTROENCEFALOGRAFO (4)	33	ANALIZZATORE MULTIPARAMETRICO A PANNELLO MISTO (PC)
6	COAGULOMETRO (PC CON GESTIONALE)	20	SPIROMETRO (PC)	34	EMOGASANALIZZATORE (1)
7	MONITOR ACQUISIZIONE IMMAGINI	21	ECOGRAFO PORTATILE	35	ANALIZZATORE AUTOMATICO PER IMMUNOCHIMICA (PC)
8	BIOBANCA (SOFTWARE)	22	ECOGRAFO (1)	36	EMOGASANALIZZATORE (2)
9	TAC (CONSOLE DI COMANDO)	23	ELETTROCARDIOGRAFO (1)	37	EMOGASANALIZZATORE (3)
10	SPETTROMETRO DI MASSA (1)	24	ELETTROCARDIOGRAFO (2)	38	CROMATOGRAFO IN FASE LIQUIDA AD ELEVATE PRESTAZIONI (PC)
11	SPETTROMETRO DI MASSA (2)	25	ECOGRAFO (2)	39	SPETTROMETRO DI MASSA CON CROMATOGRAFIA LIQUIDA (PC)
12	MODULO PER HPLC	26	ECOGRAFO (3)	40	EMOGASANALIZZATORE (4)
13	TOMOGRAFO RMN	27	ECOGRAFO (4)	41	ECOGRAFO (5)
14	WORKSTATION DI REFERTAZIONE RMN	28	ANALIZZATORE PER IMMUNOCHIMICA (PC)	42	ECOGRAFO (6)

Materials and methods – the questionnaire

- Built using Excel
- For each personal data processing in a MD, calculates an evaluation of security and privacy measures and controls actually operative and active in respect pf the three categories described above: data loss, data modification, data unlawful access
- The measures/controls considered were (yes/no)

- Anonimyzation
- Data minimization
- Physical access control
- Logical access control
- Cryptography
- Malware e sicurezza dei siti web
- Asset management
- Backup
- Manutenzione
- Contract with external processor
- Hardening
- Data storage and conservation
- Data traceability
- Partitioning
- Asset administration
- ….

Materials and methods – the questionnaire

	DISPOSITIVO	RISCHIO PER I DATI		REPARTO	OSPEDALE
1	SPETTROMETRO DI MASSA	4	MEDIO	MALATTIE METABOLICHE	BURLO
2	MODULO PER HPLC	5	MEDIO	MALATTIE METABOLICHE	BURLO
3	SPETTROMETRO DI MASSA	5	MEDIO	MALATTIE METABOLICHE	BURLO
4	SPETTROMETRO DI MASSA	4	MEDIO	MALATTIE METABOLICHE	BURLO
5	ELETTROENCEFALOGRAFO	2	BASSO	ELETTROFISIOLOGIA E NEUROPSICHIATRIA	BURLO
6	ELETTROMIOGRAFO	4	MEDIO	ELETTROFISIOLOGIA E NEUROPSICHIATRIA	BURLO
7	ELETTROENCEFALOGRAFO	3	BASSO	CARDIOLOGIA	BURLO
8	ECOTOMOGRAFO	3	BASSO	CARDIOLOGIA	BURLO
9	ECOTOMOGRAFO	4	MEDIO	CARDIOLOGIA	BURLO
10	ECOTOMOGRAFO PORTATILE	3	BASSO	CARDIOLOGIA	BURLO
11	ECOTOMOGRAFO PORTATILE	3	BASSO	PRONTO SOCCORSO	S.M. MISERICORDIA
12	ENDOSCOPIO	4	MEDIO	GASTROENTEROLOGIA	S.M. MISERICORDIA
13	ENDOSCOPIO	3	BASSO	GASTROLOGIA	BURLO
14	PIATTAFORMA DI NGS	2	BASSO	LABORATORIO	BURLO
15	TAC	4	MEDIO	RADIOLOGIA	BURLO
16	STAMPANTE RAGGI X	4	MEDIO	RADIOLOGIA	BURLO
17	APP. RADIOLOGICA	5	MEDIO	RADIOLOGIA	BURLO
18	SOFTWARE TELEMETRIA	2	BASSO	CARDIOCHIRURGIA	S.M. MISERICORDIA
19	SOFTWARE MONITORAGGIO PERFUSIONE	1	BASSO	CARDIOLOGIA	S.M. MISERICORDIA
20	SOFTWARE HOLTER	4	MEDIO	CARDIOLOGIA	S.M. MISERICORDIA

		ACCESSO DATI	MODIFICA DATI	PERDITA DATI	TOTALE MISURA DI SICUREZZA		
CONTROLLO DEGLI ACCESSI FISICI						VALORI 1	
L'apparecchiatura è in zona accessibile NON al pubblico?	SI NO					0	0,5
Per accedere all'apparecchiatura è necessario l'utilizzo di una chiave, un badge o l'inserimento di un codice?		0	0	0	0	0	0,3
Sono previste procedure di allarme nel caso in cui venga rilevato l'accesso non autorizzato ad un apparecchiatura?						0	0,2
CONTROLLO DEGLI ACCESSI LOGICI						VALORI	1
Il dispositivo è un software stand alone?						0	0
Se si:							
Il supporto dove è installato il software utilizza metodi di autenticazione per l'accesso?						0	0,4
Sono presenti metodi di autenticazione per l'accesso al software?						0	0,4
Il metodo di autenticazione utilizzato è una password?						0	0
La password è robusta?		0	0	0	0	0	0,2
Se non è un software stand alone:							
L'apparecchiatura utilizza metodi di autenticazione?						0	0,8
Il metodo di autenticazione utilizzato è una password?						0	0
La password è robusta?						0	0,3
In ogni caso:							
Dopo aver eseguito l'accesso al software o all'apparecchiatura, è impossibile modificare i dati salvati?						0	0,2

	DISPOSITIVO		VIOLAZIONE Accesso	Modifica	Perdita
1	SPETTROMETRO DI MASSA	Gravità	60,7%	54,6%	50,9%
		Probabilità	47,0%	39,0%	37,0%
2	MODULO PER HPLC	Gravità	60,7%	54,6%	50,9%
		Probabilità	47,0%	39,0%	37,0%
3	SPETTROMETRO DI MASSA	Gravità	56,8%	49,6%	44,5%
		Probabilità	51,0%	42,0%	41,0%
4	SPETTROMETRO DI MASSA	Gravità	61,8%	55,4%	51,5%
		Probabilità	44,0%	34,0%	31,0%
5	ELETTROENCEFALOGRAFO	Gravità	24,7%	26,3%	26,4%
		Probabilità	14,0%	14,0%	19,0%
6	ELETTROMIOGRAFO	Gravità	55,8%	49,7%	44,5%
		Probabilità	39,0%	34,0%	37,0%
7	ELETTROCARDIOFOGO	Gravità	45,7%	37,3%	17,3%
		Probabilità	34,0%	24,0%	10,0%
8	ECOTOMOGRAFO	Gravità	42,7%	33,8%	26,4%
		Probabilità	34,0%	24,0%	19,0%
9	ECOTOMOGRAFO	Gravità	51,0%	47,5%	40,0%
		Probabilità	34,0%	30,0%	28,0%
10	ECOTOMOGRAFO PORTATILE	Gravità	41,0%	39,6%	30,9%
		Probabilità	28,0%	24,0%	19,0%
11	ECOTOMOGRAFO PORTATILE	Gravità	38,9%	37,1%	40,0%
		Probabilità	29,4%	25,9%	30,9%
12	ENDOSCOPIO	Gravità	50,0%	50,8%	34,0%
		Probabilità	34,0%	39,0%	21,0%
13	ENDOSCOPIO	Gravità	34,0%	35,4%	19,5%
		Probabilità	26,0%	22,0%	10,0%
14	PIATTAFORMA DI NGS	Gravità	22,0%	22,3%	34,0%
		Probabilità	8,0%	9,0%	21,0%
15	TAC	Gravità	62,0%	56,5%	46,8%
		Probabilità	47,0%	39,0%	28,0%
16	STAMPANTE RAGGI X	Gravità	59,3%	53,1%	35,5%
		Probabilità	48,0%	39,0%	19,0%
17	APP. RADIOLOGICA	Gravità	72,0%	68,1%	51,4%
		Probabilità	67,0%	62,0%	46,0%
18	SOFTWARE TELEMETRIA	Gravità	32,0%	26,1%	12,7%
		Probabilità	14,0%	8,0%	1,0%
19	SOFTWARE MONITORAGGIO PERFUSIONE	Gravità	17,0%	15,0%	10,0%
		Probabilità	8,0%	9,0%	11,0%
20	SOFTWARE HOLTER	Gravità	62,2%	59,6%	49,1%
		Probabilità	39,0%	37,0%	29,0%

REGIONE AUTONOMA FRIULI VENEZIA GIULIA
istituto di ricovero e cura a carattere scientifico
Burlo Garofolo di Trieste
BURLO

Materials and methods – the REI

REI (scalar) formula

$$IVR = aX + bY + cZ + dP$$

X: DOCUMENTATION and MAINTENANCE
Y: PATIENT'S SAFETY
Z: IT SECURITY
P: PRIVACY-PIA

a,b,c,d: weights to evaluate

Materials and methods – REI risk factors and categories

DOCUMENTATION and MAINTENANCE			
TECHNICAL DOCUMENTATION	**SCHEDULED MAINTENANCE**	**CORRECTIVE MAINTENANCE IN THE LAST YEAR**	**MAINTENANCE COSTS**
FULL PRESENT (AVAILABLE WITH USER MANUAL IN ITALIAN) = 0	PM CORRECTLY MADE =0	NO = 0	GLOBAL/FULL RISK SERVICE (OR WARRANTY) = 0
PRESENT (AVAILABLE WITH USER MANUAL IN ENGLISH) = 0.5	PM MADE BUT LESS THEN ONCE IN A YEAR (OR NOT AVAILABLE OR INCOMPLETE) = 0.5	FROM 1 TO 3 OPERATIONS = 0.33	PRESENCE OF A SERVICE (i.e. ON CALL)=0.5
NOT PRESENT OR AVAIABLE = 1	AT LEAST TWO PM NOT MADE =1	FROM 4 TO 8 = 0.66	NO SERVICE =1
	NO PM OR ABSENT DOCS =1	>8 (OR ABSENT DOCUMENTATION) = 1	ABSENT OR INEXISTENT DOCS =1

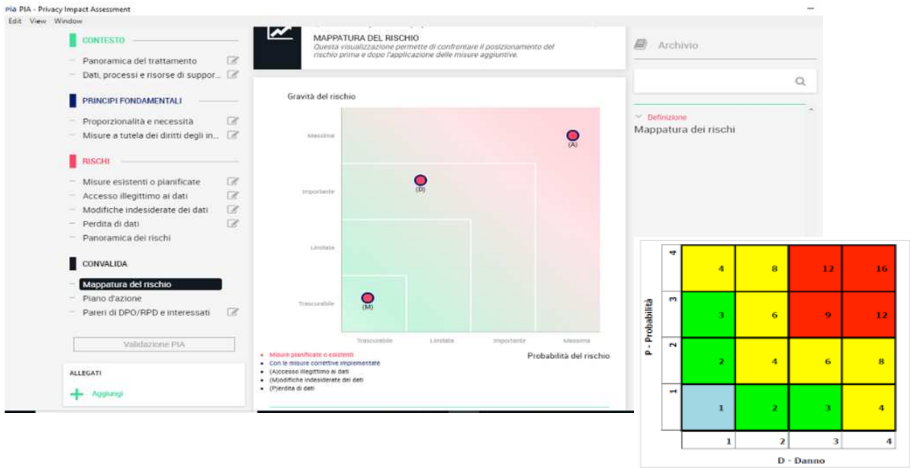
Materials and methods – REI risk factors and categories

PATIENT'S SAFETY			
INTENDED OR TARGET USE	**PATIENT'S CONSEQUENCES IN CASE OF FAILURE**	**AGE (Y)**	**UTILIZATION**
THERAPEUTIC = 1	DEATH = 1	MORE THAN 8 =1	DAILY = 1
DIAGNOSTIC = 0.66	DAMAGE = 0.75	LESS THAN 8 = 0	AT LEAST ONCE IN A WEEK = 0.75
ANALYTIC = 0.33	NOT INTENDED THERAPY = 0.5		AT LEAST ONCE IN A MONTH = 0.5
OTHER = 0	NO SIGNICATIVE RISK = 0.25		AT LEAST ONCE IN A YEAR = 0.25

Materials and methods – REI risk factors and categories

IT SECURITY						
ACCESS USERS' PASSWORDS	**ANTIVIRUS**	**BACKUP**	**VULNERABILITY TEST AND CRITICAL SITUATIONS**	**FIREWALL**	**UPS**	**SISTEMA OPERATIVO OBSOLETO**
STRONG CREDENTIALS = 0	INSTALLED AND UPDATED = 0	DAILY = 0	NO = 0	ON = 0	YES = 0	NO = 0
WEAK CREDENTIALS = 0.5	INSTALLED AND NOT UPDATED = 0.33	WEEKLY= 0.25	LOW = 0.33	OFF = 1	NO = 1	YES = 1
NOT PRESENT = 1	NOT PRESENT BUT INSTALLABLE = 0.66	MONTHLY = 0.5	MEDIUM = 0.66			
	NOT PRESENT AND NOT INSTALLABLE = 1	ANNUAL= 0.75	HIGH/TEST NOT PERFORMED= 1			
		NOT OPERATIVE= 1				

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

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.

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

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.

Results – MLR Model

REI *= aX + bY + cZ + dP*

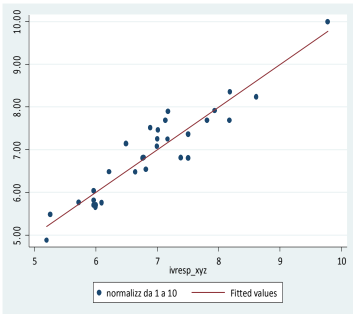
- X, vector → «*Documentation and Maintenance*»
- Y, vector → «*Patient's safety*»
- Z, vector → «*IT-security and cyber-security* »
- *P, vector* → «Privacy»

a, b, c and *d:* weights to be estimated for each risk category – multiple linear regression model

Multi-collinearity found between vectors Z and P → estimated and compared the two models respectively with X.Y and Z, and with X,Y and P

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

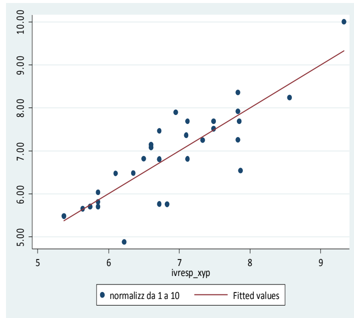


P<0.1

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

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
7.118341	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

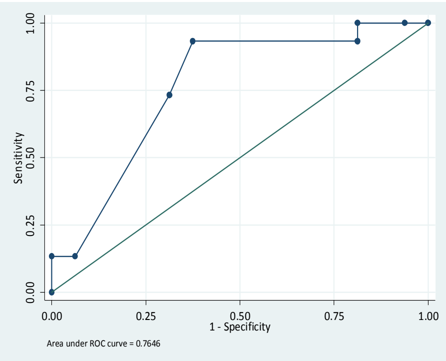
REGIONE AUTONOMA FRIULI VENEZIA GIULIA
ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO
Burlo Garofolo di Trieste
BURLO

Results – logistic model

Using Zi (IT Security) and Pi (Privacy)

Xi, Yi, Zi

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

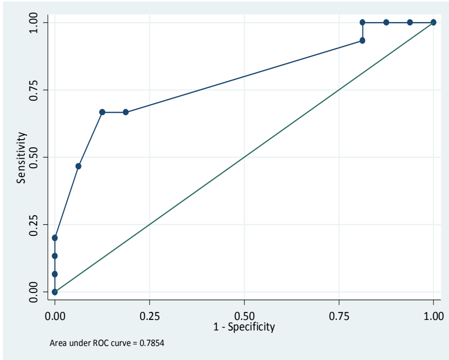


Sensitivity=93,33%
Specificity= 62,58%
Correctly classified=77,42%

P<0.15

Xi, Yi, Pi

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

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

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

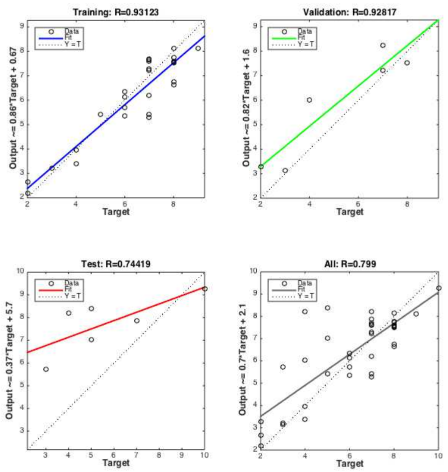
There are no significant differences in use of Zi or Pi

Neural Networks methods and results

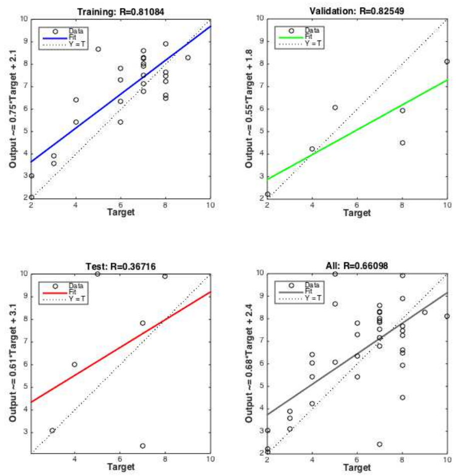
NEURAL NETWORK START - MATLAB

- 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

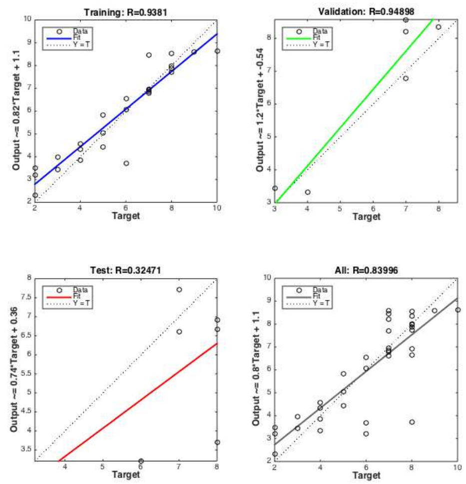
TRAINING SET : 27 of 39 MDs (the study was extended from 31 to 39 MD)
TEST SET: 6 of 39 MDs
VALIDATION SET: 6 of 39 MDs



- 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;



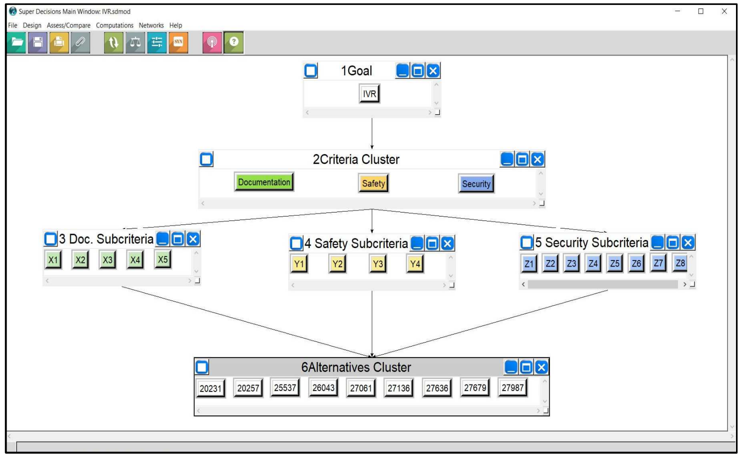
- 9 of 10 MD at low risk;
- 11 of 18 MD at medium risk;
- 8 of 11 MD at high risk;

REGIONE AUTONOMA FRIULI VENEZIA GIULIA
Istituto di Ricovero e Cura a Carattere Scientifico Burlo Garofolo di Trieste
BURLO

AHP method and results

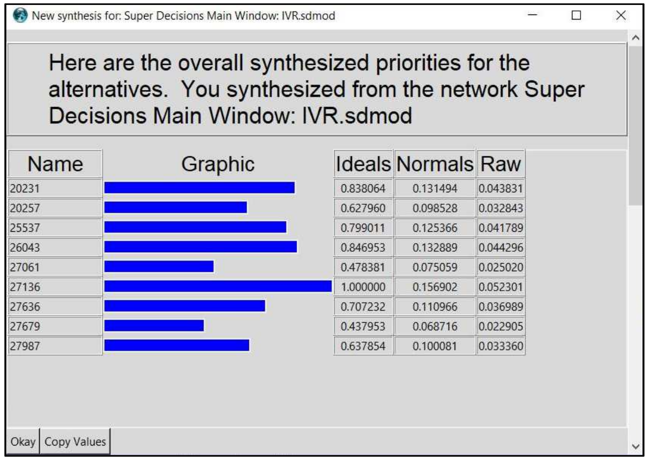
ANALYTIC HIERARCHY PROCESS

- 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

REGIONE AUTONOMA FRIULI VENEZIA GIULIA
istituto di ricovero e cura a carattere scientifico Burlo Garofolo di Trieste

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 =

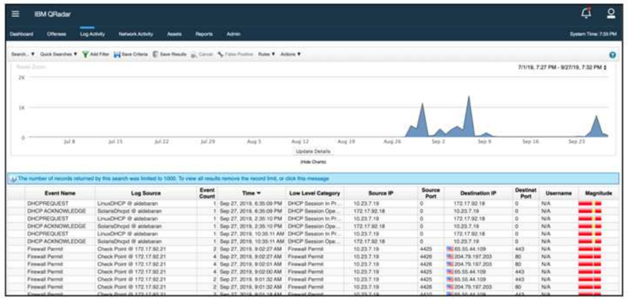
16	32	48	64	32	64	96	128	48	96	144	192	64	128	192	256
12	24	36	48	24	48	72	96	36	72	108	144	48	96	144	192
8	16	24	32	16	32	48	64	24	48	72	96	32	64	96	128
4	8	12	16	8	16	24	32	12	24	36	48	16	32	48	64
12	24	36	48	24	48	72	96	36	72	108	144	48	96	144	192
9	18	27	36	18	36	54	72	27	54	81	108	36	72	108	144
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

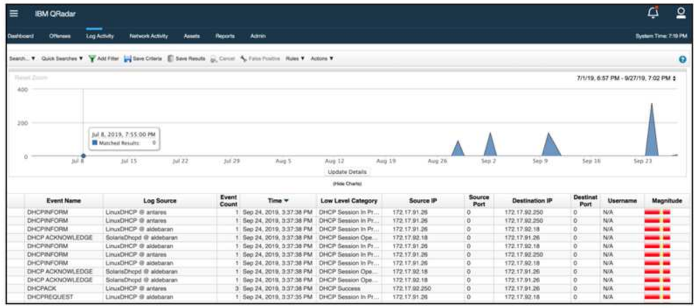
«Only» 5 MD studied; early results in MDs risk evaluation similar to the REI obtained with MLR and AHP methods

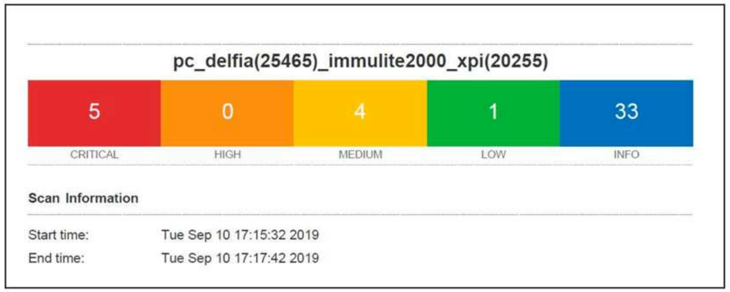
IoT Defender and early results for MD Cyber-Security

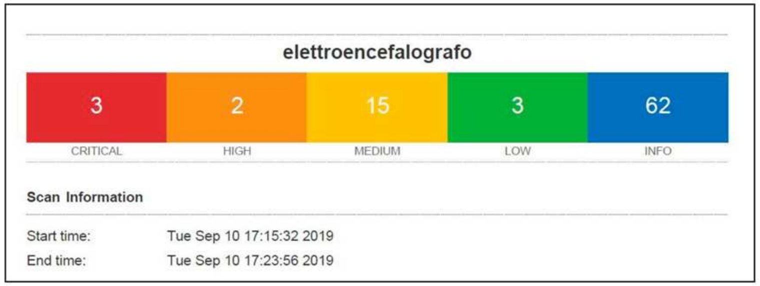
- Use of Nessus 7.1.1 Vulnerability Professional Scanner (Basic Network Scan) & Zenmap
- Traffic monitor analyzed with Qradar SIEM – IDS Sguill and Elsa/Wireshark protocol Analyzer (Kali Linux and Security Onion distribution)
- Use on MD that cannot be enforced with restrictive or controlled security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

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









REGIONE AUTONOMA FRIULI VENEZIA GIULIA
istituto di ricovero e cura a carattere scientifico
Burlo Garofolo di Trieste
BURLO

Results - discussion

Using the questionnaire, carrying out the measurements and calculating the indices it emerged that most of the MDs analyzed according to the parameters of the PIA have **medium/low risks for data loss** and **average risk for data unlawful access and data modification**, respectively.

Statistical models have allowed us to obtain values for the REI with good specificity and sensitivity, which means the obtained formula is a **fair predictive model** for the evaluation of the risks for MDs in a complex scenario such as a Hospital.

The same results highlight the **expected co-linearity** between the categories of privacy risk and IT security risk (the GDPR paradigm of data protection) and, using only privacy risk category, a representative equation was obtained at a lower computational cost and with equal results.

The early but reliable results obtained with the application of neural networks, AHP and matrix methods confirm the accuracy and repeatability of statistical methods, opening **new possibilities** in the study and research of complex integrated models for the risk analysis, evaluation and mitigation.

The preliminary results obtained using the IoT Defender device for the cybersecurity of MDs are **very promising**

Conclusions

(Healthcare) Information Security Risk Assessmnet is a multi-order and a multi-dimensional problem especially in the healthcare

Multi-order and multi-dimensional tools may be useful for the risk assessment (such as the integration of the DPIA analysis in the REI or the use of cybersecurity tools) in order to implement a predictive (or even prescriptive) analysis on the hospital MDs and track, monitor and raise the security of data on the single MD according to the EC Regulation (GDPR and the just released Cyber security Act) -> **Security & Privacy Management Model**

Smart Health, mHealth, IoHT, edge and cloud computing and all cybersecurity issues and concerns impose to risk managers the adoption of effective and reliable procedures, methods, counter-measures (ML and AI among the others), and more powerful tools to correlate events and phenomenas of a complex world.

Grazie per l'attenzione e la partecipazione

michele.bava@burlo.trieste.it

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