HEALTH TECHNOLOGY CHALLENGE AIIC 2019

# GDPR, sicurezza informatica e dispositivi medici: come la valutazione di impatto sulla protezione dei dati (PIA) impatta sul calcolo dell'indice per la valutazione dei rischi dei DM connessi ad una rete ospedaliera


**IRCCS materno-infantile «Burlo Garofolo»**
**Ospedale S.M. Misericordia - ASUIUD**

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

REGIONE AUTONOMA FRIULI VENEZIA GIULIA
PRESIDIO OSPEDALIERO UNIVERSITARIO Santa Maria della Misericordia di Udine
azienda sanitaria universitaria integrata di udine
I.M.F.R.


AIIC associazione italiana ingegneri clinici

# Il gruppo di lavoro


*Maria Chiara Corvasce*
*Dottoressa magistrale in ingegneria clinica*
*DIA – Dipartimento di Ingegneria e Architettura*
*Università degli Studi di Trieste*

*Michela Stella*
*Dottoressa magistrale in ingegneria clinica*
*DIA – Dipartimento di Ingegneria e Architettura*
*Università degli studi di Trieste*

*Ing. Riccardo Zangrando*
*Direttore SOC Ingegneria Clinica*
*Ospedale S.M.Misericordia ASUIUD*

*Ing. Massimo D'Antoni*
*Dirigente ingegnere*
*SOC Ingegneria Clinica*
*Ospedale S.M.Misericordia ASUIUD*

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

# Descrizione

Indice per la Valutazione dei Rischi dei DM & Privacy Impact Assessment

## Analisi

- ❑ GDPR e Valutazione di Impatto (PIA)
- ❑ IVR calcolato per i Dispositivi Medici: indice predittivo che include le categorie di rischio (documentazione e manutenzione, rischio per il paziente, sicurezza informatica)
- ❑ PIA del Garante è strumento tropo generico per valutazione di impatto in Sanità
- ❑ Aspetti di privacy e IT security vanno integrati e trattati assieme

## Soluzione

- ❑ Selezione di 30 DM pilota connessi alle reti IT-medicali di due ospedali/Aziende diverse del Friuli Venezia-Giulia
- ❑ Questionario che correla la valutazione di impatto con le misure previste e i rischi nelle tre sezioni del PIA: accesso illegittimo, perdita dei dati, modifica dei dati
- ❑ Integrazione della categoria di rischio «Privacy» a quelle già presenti e rimodulazione del modello dell'IVR

# Obiettivi e destinatari del lavoro

- Unificazione di procedure e metodi per la valutazione dei rischi dei DM che includano, oltre al quadro normativo proprio dei DM stessi, la sicurezza informatica e la privacy secondo il GDPR
- Creazione di un questionario che correli in modo oggettivo e ripetibile i dati provenienti dalle valutazioni di impatto dei trattamenti (nei DM, nei SW DM e/o nei SW all'interno dei DM)
  - In particolare i dati relativi ai principi di proporzionalità e necessità, ai rischi connessi al loro uso, trasmissione, ecc… e alle misure (adeguate) che sono poste in essere o che sono previste per mitigare i rischi stessi
- Destinatari:
  - i titolari delle aziende che possono rispondere in modo efficace e documentato (accountability) ad eventuali minacce
  - i manager ospedalieri, dei servizi di ingegneria clinica e dei sistemi informativi che si occupano di rischio nella più ampia accezione del termine, che possono misurare il rischio e valutare nel tempo, in modo oggettivo, l'impatto delle misure che attuano per mitigarlo
  - Agenzie pubbliche e private, opinione pubblica, servizi di monitoraggio automatici che possono tener traccia nel tempo di analisi e azioni intraprese, grazie ad un approccio nella gestione del rischio integrata e che considera aspetti diversi e complementari

# Risultati

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

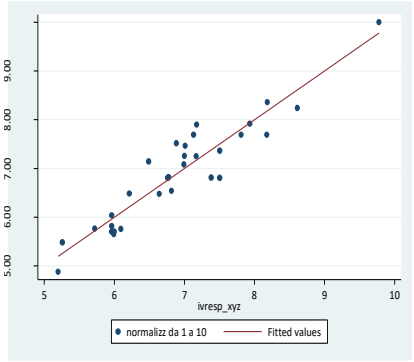
- X, vettore → «*Documentazione e Manutenzione*»
- Y, vettore → «*Rischio per il paziente*»
- Z, vettore → «*Sicurezza Informatica*»
- *P, vettore* → «Privacy»

*a, b, c e d* pesi da stimare per ciascuna categoria – modello regressione lineare multipla

Trovata multicollinearità tra Z e P → sono stati stimati e confrontati i due modelli con X.Y e Z e X,Y e 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 |

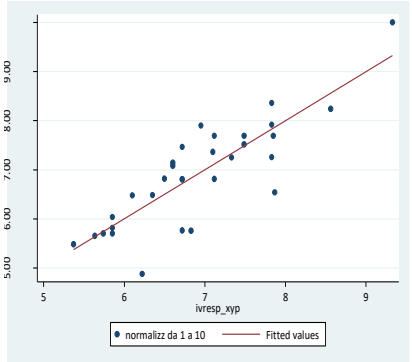
***Xi, Yi, Zi***




P<0.1

| IVR | 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

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

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

A parità di risultati (numero di DM correttamente classificati) e con un P inferiore (P<0.05), l'equazione con i Pi è computazionalmente più vantaggiosa

HEALTH TECHNOLOGY CHALLENGE AIIC 2019

# Risultati

*Ing. Michele Bava PhD*
*michele.bava@burlo.trieste.it*
*PO Informatica, Telefonia e DPO - Ufficio Sistema Informativo -*
*IRCCS materno-infantile «Burlo Garofolo»*