*Avvocato Massimiliano Parla*
***Presidente Nazionale Scudomed – Health Risk Manager e Legal Advisor***

# *COMPLIANCE e RISK MANAGEMENT* AZIENDALE

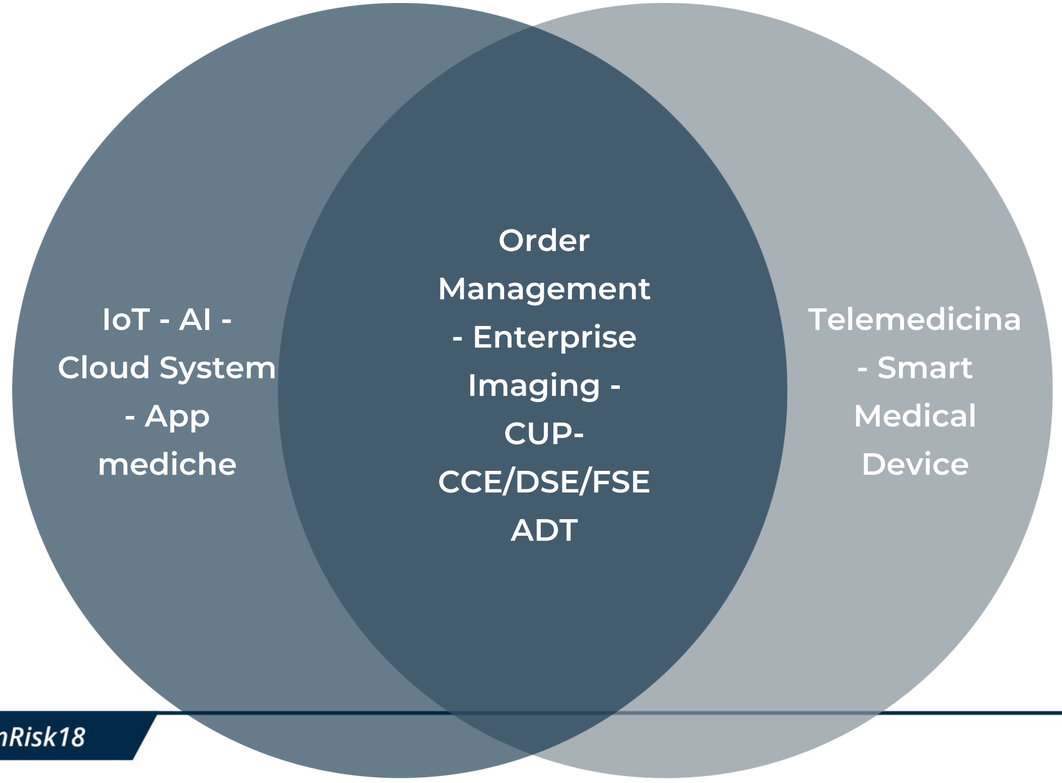
## AREZZO FORUM RISK 2023





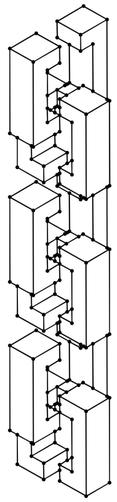
#ForumRisk18
www.forumriskmanagement.it

# SANITÀ TECNOLOGICA & DATA ENTRY




La Sanità Tecnologica e la Gestione del Rischio in Sanità non possono **oggi** non prendere in considerazione la necessaria compliance normativa in tema Cyber Security e *data protection*

- CAD 2005
- Linee Guida AgID
- DPCM 81/2021
- Framework ACN



- NIS 2 directive
- GDPR e Codice Privacy
- Iso 27001 – 27701 – 17065
- Euro Privacy Certification

# MATRIX OF APPLICABILITY

Integrazione di schemi normativi e di compliance in chiave multidisciplinare per rispondere a differenti esigenze di:

- Definizione del contesto interno ed esterno con individuazione della c.d. Supply Chain;
- Valutazione del rischio aziendale;
- Messa in Sicurezza degli Asset e delle Infrastrutture Strategiche (*core*).

21-24 NOVEMBRE 2023
AREZZO FIERE E CONGRESSI
18

# L'applicazione tecnologica in Sanità deve passare:

- Progettazione di un **perimetro** by design per i dati personali **G-Core**
- Implementazione di un **perimetro di controlli** e **sicurezza informatica**
- Attuare una **politica** definita di valutazione e di **gestione** del **rischio con ruoli e responsabilità**


## The list of criteria, and checks and controls

- Homogeneous and consistent certifications
- Divers categories of data processing activities
- GDPR Core Criteria
- Contextual checks and controls
  - Complementary contextual checks and controls
  - Technical and Organisational Measures
  - National Obligations checks and controls






#ForumRisk18

# L'ANALISI E LA VALUTAZIONE DEL RISCHIO DISTINTA PER PROCESSI

## Secondo i principi dettati dalla norme internazionali di riferimento

| id | Processo / Funzione coinvolta e singola attività sensibile | Rischio | Causa della problematica *(perché potrebbe succedere...)* | Metodo di controllo attuale *(cosa si fa per evitare che il rischio si concretizzi)* | D | P | Indice Rischio effettivo |
|---|---|---|---|---|---|---|---|
| 2 | Sicurezza delle Informazioni/Informatica | | | | | | |
| 2.3 | *Accesso alle immagini sistema RIS/PACS* | Violazione del principio RID con riguardo alle informazioni rilevanti dell'organizzazione | Mancata definizione di un perimetro di sicurezza informatica aziendale | Draft di disciplinare accessi gestionale RIS/PACS xxx - rev. x/xxxx | 4 | 4 | 16 |
| 2.4 | *Business Continuity per l'erogoazione del servizio CUP* | Interruzione nella continuità dell'attività dell'organizzazione | Incidenti di natura informatica che possono influire in merito alla corretta erogazione dei servizi istituzionali | Procedura operativa xxx - Business Continuity serv. CUP rev. x/xxxx | 4 | 2 | 8 |

*Avv. Massimiliano Parla*

*Presidente Nazionale Scudomed – Health Risk Manager*

*e Legal Advisor*

# GRAZIE PER L'ATTENZIONE

## AREZZO FORUM RISK 2023





#ForumRisk18
www.forumriskmanagement.it

**Delitti in materia di violazione del diritto d'autore (Art. 25-novies, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 99/2009]**

- Messa a disposizione del pubblico, in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta, o di parte di essa (art. 171, legge n.633/1941 comma 1 lett. a) bis)
- Reati di cui al punto precedente commessi su opere altrui non destinate alla pubblicazione qualora ne risulti offeso l'onore o la reputazione (art. 171, legge n.633/1941 comma 3)
- Abusiva duplicazione, per trarne profitto, di programmi per elaboratore; importazione, distribuzione, vendita o detenzione a scopo commerciale o imprenditoriale o concessione in locazione di programmi contenuti in supporti non contrassegnati dalla SIAE; predisposizione di mezzi per rimuovere o eludere i dispositivi di protezione di programmi per elaboratori (art. 171-bis legge n.633/1941 comma 1)
- Riproduzione, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico, del contenuto di una banca dati; estrazione o reimpiego della banca dati; distribuzione, vendita o concessione in locazione di banche di dati (art. 171-bis legge n.633/1941 comma 2)
- Abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico con qualsiasi procedimento, in tutto o in parte, di opere dell'ingegno destinate al circuito televisivo, cinematografico, della vendita o del noleggio di dischi, nastri o supporti analoghi o ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento; opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico musicali, multimediali, anche se inserite in opere collettive o composite o banche dati; riproduzione, duplicazione, trasmissione o diffusione abusiva, vendita o commercio, cessione a qualsiasi titolo o importazione abusiva di oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi; immissione in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa (art. 171-ter legge n.633/1941)
- Mancata comunicazione alla SIAE dei dati di identificazione dei supporti non soggetti al contrassegno o falsa dichiarazione (art. 171-septies legge n.633/1941)
- Fraudolenta produzione, vendita, importazione, promozione, installazione, modifica, utilizzo per uso pubblico e privato di apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale (art. 171-octies legge n.633/1941).

**Torna all'inizio**