AIIC 2025 CONVEGNO NAZIONALE ASSOCIAZIONE ITALIANA INGEGNERI CLINICI

NAPOLI 14-17 GIUGNO 2025 MOSTRA D'OLTREMARE

AIIC associazione italiana ingegneri clinici

La normativa regolatoria: dal GDPR alla NIS 2 *un percorso che prosegue*

Graziano de' Petris

DPO Sanità, PdC NIS 2, Vicepresidente A

ATORI

TECNOLOGIE, SOSTENIBILITÀ, AMBIENTE
Il contributo dell'innovazione alla sanità del futuro

Obiettivi di questa lezione

- Comprendere le sinergie e i punti di contatto tra il GDPR e la Direttiva NIS 2
- Apprendere le novità introdotte dalla L. 90/2024 e dal D.Lgs. 138/2024 in relazione alla gestione dei Dispositivi Medici (DM).
- Distinguere i ruoli e le responsabilità del Referente per la Cybersecurity (RpC), del Chief Information Security Officer (CISO) del Punto di Contatto NIS 2 (PdC) del Responsabile della Transizione digitale (RTD) e del Data Protection Officer (DPO).
- Valutare l'impatto di queste normative sul proprio lavoro quotidiano e sulle strategie di sicurezza delle Aziende sanitarie.

il 9 gennaio 2007 Steve Jobs presenta

È stato l'inizio di una nuova era

con i suoi pro e i suoi contro

da quel momento il mondo non è più quello di prima

È finita l'era dell'Ingegnere Clinico che si preoccupa soltanto della sicurezza elettrica e meccanica *perché tutto il resto è roba da informatici*

Anch
veco
evo

Le regole sono in continua evoluzione *da molti anni*

in Europa il panorama regolatorio in materia di cybersicurezza e protezione dei dati

è in continua evoluzione da prima delle prime linee guida AgID (2017)

normative sempre più stringenti

mirano a rafforzare la resilienza digitale di aziende e organizzazioni

dal GDPR alla NIS 2, passando per l'IA ACT, il Regolamento MD

e in Italia le linee guida AgID, la L 90/2024, il dlgs 138/2024

l'obiettivo è quello di creare un ambiente digitale più sicuro e affidabile

Un breve ripasso del GDPR

- **Principi fondamentali:** liceità, correttezza, trasparenza, minimizzazione, esattezza, limitazione della conservazione, integrità e riservatezza (sicurezza), accountability (rendicontazione).
- **Concetti chiave:** Dati Personali, Dati particolari (7 categorie), Titolare, Responsabile del Trattamento, Autorizzati al trattamento. Diritti degli interessati esercitabili autonomamente (rendicontazione all'interessato).
- **Art. 25** Data Protection by design e by default
- **Art. 32** (Sicurezza del trattamento): misure tecniche e organizzative adeguate al rischio.
- **Notifica delle violazioni** (Data Breach): tempistiche strette (72 ore) e autorità competente (Garante

Esempio pratico

un tecnico della manutenzione smarrisce una chiavetta USB **non crittografata** contenente dati anonimizzati di test di un dispositivo medico, comunque in qualche modo riconducibili ai pazienti.

obbligo di attivare la procedura di data breach

anche se non è un dato diretto, il Garante ne chiede conto e solitamente sanziona

Il Framework del GDPR e il principio fondamentale della Security by Design

Il GDPR è stato impostato su un nuovo approccio alla protezione dei dati, **basato sul rischio** e sui principi di **responsabilizzazione** e di **protezione dei dati sin dalla progettazione e per impostazione predefinita**

gli articoli 24, 25, 29, 32 e 33, introducono un framework completo per la gestione della sicurezza informatica

l'art. 25 sancisce i principi della data protection by design e by default

l'articolo 32 stabilisce i requisiti fondamentali per garantire un livello di sicurezza "adeguato al rischio«

il principio enunciato nel Considerando 83 , sottolinea la necessità di una valutazione dei rischi intrinseci al trattamento.

Il Considerando 74 enfatizza la **responsabilità del titolare del trattamento** nell'adozione di adeguate **politiche interne di gestione e tutela dei dati** e nell'attuazione di misure che soddisfino i principi della *data protection by design e by default*.

Troviamo un riscontro diretto nelle prescrizioni tecniche della Direttiva (UE) NIS2 e già prima nelle vostrane misure minime di sicurezza AgID che possiamo interpretare come una codificazione operativa di questi principi

La chiara correlazione tra le misure AgID e i requisiti GDPR

Le misure minime di sicurezza ICT emanate dall'AgID rappresentano a tutti gli effetti una traduzione pratica dei requisiti di sicurezza delineati dall'articolo 32 del GDPR.

In particolare:

- l'inventario dei dispositivi e dei software autorizzati corrisponde alla "capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi" (Art. 32, par. 1, lett. b);
- le procedure di configurazione sicura riflettono il principio di "protezione dei dati fin dalla progettazione" (Art. 25);
- il monitoraggio continuo e la gestione degli incidenti implementano operativamente l'obbligo di notifica delle violazioni (Art. 33).

Il Perimetro di Sicurezza Nazionale nel Contesto del GDPR

Il Perimetro di Sicurezza Nazionale Cibernetica, istituito dal DL 105/2019, non rappresenta altro che una specializzazione settoriale dei principi di sicurezza del GDPR. Come evidenziato dal Considerando 85, la necessità di prevenire danni e pregiudizi agli interessati si traduce nella necessità di:

- requisiti di *procurement* sicuro, che implementano il rispetto del principio di *accountability* dell'Art. 24;
- procedure di *incident handling*, che sono perfettamente allineate con gli obblighi dell'Art. 33;
- misure di protezione delle infrastrutture critiche, che concretizzano il requisito di "resilienza" dell'Art. 32.

L. 90/2024 e D.Lgs. 138/2024: cosa cambia nella gestione dei DM

Contesto normativo italiano:

- L. 90/2024 (Legge di conversione del D.L. 19/2024) > attenzione crescente del legislatore nazionale alla cybersicurezza, in linea con l'implementazione NIS 2
- **D.Lgs. 138/2024** (Attuazione della Direttiva NIS 2)

I Dispositivi Medici (DM) nell'ambito NIS 2 sono critici!

interconnessi, potenziale impatto sulla salute e sulla vita dei pazienti, varie possibili vulnerabilità

Cosa significa per l'Ingegnere clinico dell'Azienda Sanitaria

Inclusione dei fabbricanti di DM tra i "Soggetti Essenziali" o "Soggetti Importanti" (settore "tecnologie sanitarie").

- **Responsabilità del fabbricante:** Obblighi di sicurezza nel ciclo di vita del DM (dalla progettazione alla dismissione), inclusa la sicurezza del software e degli aggiornamenti.
- **Impatto sull'approvvigionamento:** Necessità di valutare la sicurezza informatica dei DM anche in fase di acquisto/gara. Necessità di clausole contrattuali specifiche.
- **Gestione del rischio dei DM in uso:** L'azienda sanitaria è responsabile della sicurezza dei DM che acquista e utilizza. Come integrare i requisiti NIS 2 nella gestione del parco DM esistente e nuovo?.
- **Vulnerabilità e patch:** Gestione proattiva delle vulnerabilità note e applicazione delle patch fornite dai fabbricanti.
- **Notifica incidenti:** L'azienda sanitaria deve notificare gli incidenti significativi che coinvolgono i DM (se rientra nel perimetro NIS 2 come struttura sanitaria) anche all'ACN, oltre che al Garante Privacy

Esempio pratico

Un nuovo ventilatore polmonare connesso in rete deve essere stato progettato e realizzato "security by design "

Deve avere le porte di comunicazione protette, autenticazione informatica robusta

Deve essere previsto un piano chiaro di aggiornamenti di sicurezza fornito dal fabbricante

non basta più che sia "funzionale"

Le «nuove» misure di sicurezza

Art. 21 del D.Lgs. 138/2024 *si applicabilità anche ai DM.*

Esempi concreti per i DM:

- **Segmentazione** della rete per isolare i DM.
- **Autenticazione** forte per l'accesso ai DM.
- **Backup** e piani di **ripristino** specifici per i sistemi legati ai DM.
- **Sicurezza della catena di fornitura** (anche per i DM e i loro componenti).
- **Formazione** specifica per gli operatori sui rischi dei DM connessi.

L’impatto sull'approvvigionamento (supply chain) è importante!

È indispensabile saper valutare la sicurezza informatica dei DM anche in fase di acquisto/gara.

Bisognerà richiedere la conformità NIS 2 ai fornitori con **Clausole contrattuali specifiche**!

Esempio pratico

In un capitolato d'appalto per l'acquisto di nuove pompe infusionali intelligenti, l'ingegnere clinico dovrà includere requisiti che attestino la capacità del fabbricante di gestire le vulnerabilità software, fornire patch di sicurezza e documentare la resilienza del dispositivo agli attacchi informatici.

La gestione dei DM

- **Gestione del rischio dei DM in uso:** L'azienda sanitaria è responsabile della sicurezza dei DM che acquista e utilizza. Bisogna integrare i requisiti NIS 2 nella gestione del parco DM esistente e nuovo. Questa attività include la lettura dei **Medical Device Security Bulletins**.

- **Vulnerabilità e patch:** è necessario gestire proattivamente le vulnerabilità note e applicare le patch fornite dai fabbricanti (o fargliele applicare).

Esempio pratico

Viene emesso un avviso di sicurezza (alert) per una vulnerabilità critica in un modello specifico di risonanza magnetica connessa

L'ingegnere clinico dovrà collaborare con l'IT e il fabbricante per valutare il rischio, pianificare e implementare la patch o le mitigazioni necessarie, **garantendo la continuità del servizio e la sicurezza del paziente**

La notifica degli incidenti

Se l'Azienda rientra nel perimetro NIS 2 come struttura sanitaria, deve notificare gli incidenti significativi che coinvolgono i DM anche all'ACN, oltre che al Garante Privacy se c'è un data breach.

Focalizziamoci sulla Direttiva NIS 2

- **Obiettivi:** rafforzare la cybersicurezza nell'UE e aumentare la resilienza dei settori critici.
- **Ampliamento** dell'ambito di applicazione rispetto alla NIS 1 (più settori critici, inclusa la sanità e i fabbricanti di DM).
- **Concetti chiave:** Soggetti Essenziali e Soggetti Importanti.
- **Misure di gestione dei rischi** di cybersicurezza (Art. 21 D.Lgs. 138/2024): un elenco più prescrittivo rispetto al GDPR (es.

La NIS2 vista come un'estensione operativa del GDPR

In quest'ottica, la Direttiva NIS2 può essere interpretata come un'estensione operativa dei principi di sicurezza del GDPR, evidenziati dal Considerando 78, che enfatizza la necessità di misure tecniche e organizzative appropriate. In particolare:

- I requisiti di *risk management* enunciati dalla NIS2 rispecchiano l'approccio basato sul rischio dell'Art. 32 GDPR;
- Gli obblighi di reporting degli incidenti si allineano con l'Art. 33 GDPR;
- Le misure di *supply chain security* implementano il principio di responsabilizzazione del titolare dell'Art. 24.

Sinergie e punti di contatto

- **Approccio basato sul rischio:** Entrambe richiedono una valutazione e gestione del rischio per le rispettive finalità.
- **Misure tecniche e organizzative:** Spesso sovrapponibili (es. sistemi di accesso, crittografia, backup). La NIS 2 fornisce requisiti più dettagliati in ambito cybersecurity.
- **Gestione e Notifica degli Incidenti:**
  - GDPR: notifica al Garante se c'è violazione di dati personali.
  - NIS 2: notifica all'ACN per incidenti significativi che compromettono la continuità dei servizi.
  - Casi di sovrapposizione: un attacco ransomware può essere sia un incidente NIS 2 che un data breach GDPR. Necessità di coordinamento tra ACN e Garante.
- **Accountability e Responsabilità del Management:** Entrambe enfatizzano la responsabilità del vertice aziendale (Art. 23 D.Lgs. 138/2024 per NIS 2).
- **Formazione e consapevolezza:** Cruciale per entrambe le normative per ridurre il rischio umano.

Esempio pratico

Un'azienda sanitaria deve valutare il rischio di un attacco ransomware (rischio NIS 2) che potrebbe rendere inaccessibili i dati dei pazienti (rischio GDPR)

Le misure preventive per la sicurezza dei sistemi (NIS 2) proteggeranno di conseguenza anche i dati personali (GDPR).

Collegamenti tra GDPR e NIS 2 1/3

il **Regolamento Generale sulla Protezione dei Dati (GDPR)** e la **Direttiva NIS 2 (Network and Information Security 2)** due pilastri fondamentali della normativa europea con obiettivi *in apparenza* distinti

sinergie e punti di contatto:

- **Approccio basato sul rischio (Risk-based approach):** Entrambe le normative adottano un approccio basato sul rischio. Il GDPR richiede che le misure di sicurezza siano proporzionate al rischio per i diritti e le libertà delle persone fisiche, mentre la NIS 2 impone alle organizzazioni di adottare misure di gestione dei rischi di cybersicurezza per prevenire e minimizzare l'impatto degli incidenti.

- **Responsabilità del vertice aziendale:** Sia il GDPR che la NIS 2 sottolineano la responsabilità del top management. Nel GDPR, il titolare del trattamento deve garantire l'applicazione delle misure di sicurezza e dimostrarne l'efficacia (principio di *accountability*). La NIS 2, in particolare con l'articolo 23 del D.Lgs. 138/2024, esplicita che gli organi di amministrazione **e direttivi** devono supervisionare direttamente l'implementazione delle misure di sicurezza e seguire una formazione specifica in materia di cybersecurity.

Collegamenti tra GDPR e NIS 2 2/3

- **Gestione degli incidenti e notifica:** Entrambe le normative prevedono obblighi di notifica degli incidenti. Il GDPR impone la notifica al Garante per la Protezione dei Dati Personali entro 72 ore in caso di violazione dei dati personali. La NIS 2 richiede la notifica degli incidenti significativi alle autorità competenti (in Italia, l'ACN - Agenzia per la Cybersicurezza Nazionale) entro tempistiche precise (pre-notifica entro 24 ore, notifica dettagliata entro 72 ore e relazione finale entro un mese). In caso di incidenti che coinvolgano anche dati personali, è fondamentale che le autorità competenti (ACN e Garante Privacy) cooperino per evitare duplicazioni di sanzioni.
- **Misure tecniche e organizzative:** Le misure di sicurezza spesso si intersecano. Ad esempio, un robusto sistema di gestione degli accessi o un firewall ben configurato proteggono sia i dati personali (GDPR) che le reti e i sistemi informatici (NIS 2). La NIS 2, inoltre, impone misure di sicurezza più stringenti come l'autenticazione a più fattori, la segmentazione della rete, la protezione da malware, il backup regolare dei dati e la sicurezza del ciclo di vita del software.

GDPR: notifica al Garante entro 72 ore dalla violazione di dati personali.

Collegamenti tra GDPR e NIS 2 3/3

- **Sistemi documentali, verifiche e audit:** Sia il GDPR che la NIS 2 richiedono l'implementazione di sistemi documentali, verifiche e audit per dimostrare la conformità e l'efficacia delle misure adottate.

- **Sensibilizzazione e formazione:** La formazione del personale è un elemento chiave in entrambe le normative, fondamentale per creare una cultura della sicurezza e ridurre il rischio di incidenti dovuti a errori umani.

GDPR e NIS 2 non sono norme esclusive, **sono complementari**

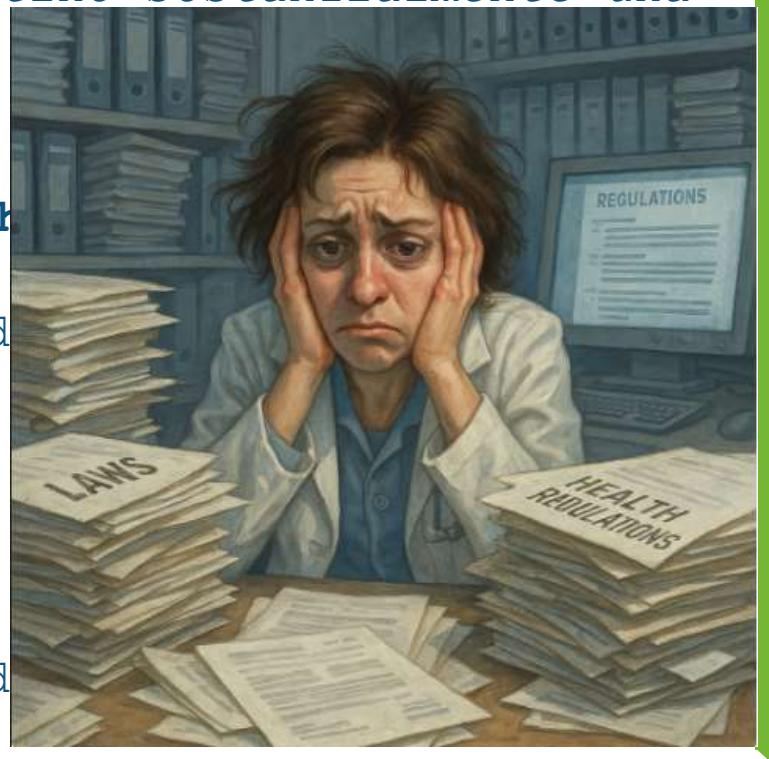
richiedono alle organizzazioni di adottare strategie coordinate

per la gestione delle minacce digitali ai sistemi di gestione e alle informazioni trattate

richiedono un approccio olistico alla cybersecurity e alla protezione dei dati

La Convergenza Operativa delle Normative

L'analisi delle sovrapposizioni normative rivela come i requisiti specifici di NIS2, AgID e del Perimetro di Sicurezza rappresentino sostanzialmente una declinazione operativa dei principi GDPR.
Infatti l'Ingegnere Clinico ha a che fare con:



Il principio di accountability GDPR (Art. 24) ch
- nei Requisiti di governance della NIS 2
- nelle Strutture organizzative del Perimetro d
- nel Framework di compliance AgID

La Data protection by Design GDPR (Art. 25) che
- nei Requisiti di *secure design* della NIS 2
- nelle Misure minime di configurazione AgID
- nelle Specifiche di sicurezza del Perimetro d

Gli obblighi di sicurezza GDPR (Art. 32) che si concretizzano:
- nei Controlli tecnici della NIS 2
- nelle Misure minime AgID
- nei Requisiti di resilienza del Perimetro di Sicurezza

Implicazioni Pratiche

La complessità del quadro normativo italiano in materia di *cybersecurity*
può essere compresa meglio interpretando le varie normative
come specificazioni operative dei principi fondamentali del GDPR

Questa lettura unificante offre vantaggi significativi in termini di:

- **Semplificazione** dell'approccio alla compliance
- **Ottimizzazione** degli investimenti in sicurezza
- **Coerenza** nell'implementazione delle misure di protezione

Sovrapposizioni e necessità di coordinamento

Scenario: Un **attacco ransomware** cripta i server del PACS, rendendo inaccessibili le immagini diagnostiche dei pazienti.

- **Obbligo NIS 2:** L'incidente compromette la disponibilità di un servizio essenziale (diagnostica per immagini). Notifica immediata all'**ACN**.

- **Obbligo GDPR:** Se l'attacco ha permesso l'accesso non autorizzato ai dati personali contenuti nel PACS (anche se criptati), o se i dati sono stati distrutti/alterati, si configura un **Data Breach**. Notifica al **Garante Privacy**.

*In questi casi è fondamentale che l'organizzazione disponga di **procedure chiare** [illegible] mantenendo la*

Accountability (mettersi in grado di poter rendicontare)

- **Accountability e Responsabilità del Management:** entrambe enfatizzano la responsabilità del vertice aziendale (**Art. 24 GDPR** e **Art. 23 D.Lgs. 138/2024** per NIS 2). I vertici devono partecipare attivamente e non delegare solo la responsabilità operativa.
- **Formazione e consapevolezza:** cruciale per entrambe le normative per ridurre il rischio umano. *Ogni ingegnere clinico che interagisce con sistemi informatici sanitari* ***deve*** *essere consapevole dei rischi.*

L. 90/2024 e D.Lgs. 138/2024 *cosa cambia nella gestione dei DM?* 1/3

La **Legge 90/2024** (Legge 23 maggio 2024, n. 90, di conversione del D.L. 19/2024), non è la normativa che recepisce rirrettamente la NIS2, MA introduce alcune disposizioni volte al rafforzamento del quadro normativo in materia di cybersicurezza, in vista e in coerenza con le nuove direttive europee.

Il **Decreto Legislativo 138/2024** (Decreto Legislativo 13 giugno 2024, n. 138, di attuazione della Direttiva NIS 2) ha un impatto significativo anche sul settore dei Dispositivi Medici (DM). **Questo è il testo chiave**

dall'entrata in vigore del D.Lgs. 138/2024, il settore dei Dispositivi Medici si è trovato ad affrontare

nuovi obblighi particolarmente stringenti in materia di cybersicurezza

ora anceh i fabbricanti dei dispositivi rientrano tra i "soggetti essenziali" o "importanti" della Direttiva NIS 2

L. 90/2024 e D.Lgs. 138/2024 *cosa cambia nella gestione dei DM?* 2/3

- **Ampliamento dell'ambito di applicazione:** A differenza della precedente Direttiva NIS, la NIS 2 estende gli obblighi di cybersicurezza ai fabbricanti di dispositivi medici, riconoscendo la loro criticità per la salute e la sicurezza dei pazienti. In base al D.Lgs. 138/2024, le aziende che producono dispositivi medici o diagnostici destinati a infrastrutture critiche (es. ospedali) o che operano su larga scala rientrano tra i soggetti essenziali. Le aziende con almeno 50 dipendenti o 10 milioni di fatturato e che operano nel settore "tecnologie sanitarie" possono rientrare tra i soggetti importanti.
- **Obblighi di cybersicurezza specifici:** I fabbricanti di dispositivi medici devono adottare misure tecniche e organizzative adeguate per la gestione dei rischi di cybersicurezza, tenendo conto delle vulnerabilità specifiche dei dispositivi medici e della loro interconnessione. Ciò include la sicurezza del ciclo di vita del software integrato nei dispositivi, dall'ideazione alla dismissione. Le misure da adottare sono esplicitamente indicate nell'art. 21 del D.Lgs. 138/2024 e comprendono, tra le altre: politiche di analisi dei rischi e di sicurezza dei sistemi informativi, gestione degli incidenti, gestione della continuità operativa, sicurezza della catena di fornitura, sicurezza nell'acquisizione, sviluppo e manutenzione di reti e sistemi informativi, test periodici, uso di crittografia e autenticazione a più

L. 90/2024 e D.Lgs. 138/2024 *cosa cambia nella gestione dei DM?* 3/3

- **Notifica degli incidenti:** Diventa obbligatoria la notifica degli incidenti di cybersicurezza significativi che coinvolgono i dispositivi medici alle autorità competenti (ACN). I tempi sono stringenti: pre-notifica entro 24 ore dalla conoscenza dell'incidente, notifica dettagliata entro 72 ore e relazione finale entro un mese.
- **Formazione e sensibilizzazione:** È richiesto un impegno costante nella formazione del personale coinvolto nella progettazione, produzione e manutenzione dei dispositivi, per riconoscere e gestire le minacce informatiche.
- **Responsabilità del management:** Il D.Lgs. 138/2024 pone una chiara responsabilità in capo agli organi di amministrazione e direzione per la supervisione e l'implementazione delle misure di cybersicurezza. Questi devono anche seguire corsi di formazione per acquisire conoscenze adeguate.
- **Tempistiche di adeguamento:** Il D.Lgs. 138/2024 prevede tempistiche specifiche per l'adeguamento: 9 mesi dalla comunicazione dell'ACN di essere identificati come soggetto NIS 2 per gli obblighi di notifica degli incidenti e 18 mesi per gli obblighi relativi alle misure da adottare e quelli in capo agli organi di amministrazione e direzione.

L'obiettivo

garantire un elevato livello di sicurezza informatica per MD, SW e infrastrutture di rete

minimizzando i rischi di attacchi informatici

per proteggere la salute dei pazienti

è fondamentale la collaborazione dell'IC non solo con IT, Qualità, Acquisti, Legale e «Privacy»

facile a dirsi!

ma anche con CISO, PdC, RTD e DPO per una gestione olistica della cybersicurezza e della protezione delle informazioni (dei dati). È fondamentale una **vision strategica** della **Direzione aziendale** che metta a sistema all'interno dell'organizzazione sanitaria detta collaborazione attraverso protocolli operativi ad hoc!

I ruoli del CISO, del Referente della Cybersecurity, del Punto di Contatto, del RTD e del DPO

Le figure chiave nel contesto della cybersicurezza aziendale ruoli e responsabilità specifiche:

- **Il Chief Information Security Officer (CISO):**
  - **Ruolo strategico:** Il CISO è la figura di riferimento per la sicurezza informatica a livello strategico e manageriale. Riporta spesso direttamente al CEO o al Board, garantendo indipendenza e visibilità.
  - **Responsabilità:** Definisce e implementa la strategia di cybersecurity dell'azienda, coordina il framework di governance della sicurezza delle informazioni, garantisce la conformità normativa (GDPR, NIS 2, ISO 27001), valuta e gestisce i rischi informatici, supervisiona la risposta agli incidenti, gestisce i piani di disaster recovery e business continuity.
  - **Competenze:** Oltre a competenze tecniche avanzate, il CISO deve possedere capacità manageriali, di leadership, di comunicazione e di gestione del team. Promuove la cultura della sicurezza in azienda attraverso formazione e sensibilizzazione del personale.

Il Referente della Cybersecurity (o Responsabile della Sicurezza, CSO - Chief Security Officer)

- **Ruolo operativo/esecutivo:** Questa figura si occupa principalmente dell'implementazione operativa delle misure di sicurezza stabilite a livello strategico dal CISO o dal management. Può essere una risorsa interna o un consulente esterno.
- **Responsabilità:** Può essere responsabile della gestione quotidiana dei sistemi di sicurezza, del monitoraggio delle minacce, dell'applicazione delle patch di sicurezza, della gestione delle vulnerabilità e del supporto tecnico per le problematiche di cybersecurity.
- **Interazione:** Collabora strettamente con il CISO per tradurre le strategie in azioni concrete e con il punto di contatto per le comunicazioni operative. In organizzazioni più piccole, il ruolo di referente della cybersecurity può essere svolto dal CISO stesso o da un altro responsabile IT.

Esempi Pratici

Il CISO Aziendale definisce una politica che impone l'uso di autenticazione a più fattori su tutti i sistemi che gestiscono dati sanitari, *inclusi i software di gestione dei DM*.

Il Referente della Cybersecurity Aziendale lavora a stretto contatto con l'ingegnere clinico e con il responsabile ICT per configurare i firewall e le VPN che proteggono l'accesso remoto ai DM e per implementare le patch di sicurezza raccomandate per i sistemi operativi dei dispositivi medici.

Il Punto di Contatto (NIS 2)

- **Il Punto di Contatto (NIS 2):**
  - **Ruolo di interfaccia:** Il punto di contatto è una persona fisica o giuridica designata dall'organizzazione come interlocutore ufficiale con l'Agenzia per la Cybersicurezza Nazionale (ACN) per le comunicazioni relative alla NIS 2. L'ACN fornirà un sistema sicuro per le comunicazioni.
  - **Responsabilità:** Gestisce l'accesso e l'aggiornamento dei dati sulla piattaforma ACN, coordina le notifiche di incidente di sicurezza informatica all'ACN (entro le tempistiche previste: 24h, 72h, 1 mese), e supervisiona gli aspetti legati alla sicurezza informatica dell'organizzazione in relazione agli obblighi NIS 2. È il canale ufficiale per le richieste di informazioni e per le notifiche da parte dell'ACN.
  - **Delegabilità:** La normativa consente di assegnare il ruolo al rappresentante legale, a un procuratore generale con adeguati poteri o a un dipendente delegato. La responsabilità finale della conformità rimane comunque in capo agli organi di amministrazione.

Il Data Protection Officer (GDPR artt. 37-39)

Il Data Protection Officer (DPO | Responsabile per la Protezione dei Dati) riveste un ruolo di fondamentale importanza nel settore sanitario, considerata la particolare sensibilità dei dati trattati e la complessità e velocità di evoluzione della normativa del settore.

- **Ruolo del DPO in Sanità: i**l DPO sanitario funge da punto di riferimento interno ed esterno per tutte le questioni relative alla protezione dei dati personali. Opera come figura di raccordo tra l'organizzazione sanitaria, i pazienti e le autorità di controllo, garantendo che il trattamento dei dati avvenga nel rispetto del GDPR e della normativa nazionale specifica del settore sanitario. Le sue **Responsabilità Principali** riguardano:

- **Controllo e monitoraggio della conformità:** Il DPO deve verificare costantemente che l'azienda sanitaria rispetti il GDPR, il Codice Privacy italiano e le normative specifiche del settore sanitario. Questo include la supervisione dei trattamenti di dati relativi alla salute, che richiedono particolare attenzione essendo categorie speciali di dati personali.

- **Valutazione d'impatto sulla protezione dei dati (DPIA):** Deve coordinare e supervisionare le valutazioni d'impatto per i trattamenti ad alto rischio, particolarmente frequenti in ambito sanitario a causa dell'uso di nuove

Il Data Protection Officer (GDPR artt. 37-39)

2/3

- **Registro delle attività di trattamento**: ne garantisce la tenuta e l'aggiornamento, documentando tutte le operazioni sui dati personali.

- **Data breach**: coordina le procedure di gestione dei *data breach*, dalla rilevazione alla notifica all'autorità e agli interessati.

- **Formazione e sensibilizzazione**: Ha la responsabilità di progettare e implementare programmi formativi specifici per il personale sanitario, amministrativo e tecnico, considerando le peculiarità del trattamento dati in sanità.

- **Gestione delle richieste degli interessati**: Coordina le procedure per gestire l'esercizio dei diritti dei pazienti, come l'accesso, la rettifica, la cancellazione e la portabilità dei dati sanitari, tenendo conto delle specificità normative del settore.

- **Punto di contatto con l'Autorità Garante**: Rappresenta l'interfaccia principale con il Garante per la protezione dei dati personali per tutte le questioni relative ai trattamenti sanitari.

Il Data Protection Officer (GDPR artt. 37-39)

Competenze Specifiche Richieste al DPO

- **Conoscenze giuridiche specialistiche:** oltre alla padronanza del GDPR, deve conoscere approfonditamente il Codice Privacy, le Linee Guida del Garante sui trattamenti sanitari, le normative regionali sanitarie e la deontologia delle professioni sanitarie.
- **Competenze tecniche e informatiche:** deve comprendere le architetture dei sistemi informativi sanitari, le tecnologie di telemedicina, i dispositivi medici connessi, la cybersecurity sanitaria e le modalità di conservazione e trasmissione sicura dei dati.
- **Conoscenze organizzative sanitarie:** è essenziale la comprensione dell'organizzazione sanitaria, dei processi assistenziali, delle dinamiche multidisciplinari e delle interazioni tra diversi attori del sistema sanitario.
- **Capacità di risk management:** deve saper identificare, valutare e gestire i rischi specifici legati ai trattamenti di dati sanitari, considerando sia gli aspetti privacy che quelli di sicurezza informatica.
- **Competenze comunicative e relazionali:** deve saper interagire efficacemente con professionisti sanitari, pazienti, direzioni aziendali e autorità di controllo, adattando il linguaggio tecnico-giuridico ai diversi interlocutori.
- Il DPO sanitario deve inoltre mantenere un aggiornamento costante sulle [illegible], partecipando a corsi di formazione specialistici e confrontandosi con le best practice del

In sintesi

il **CISO** ha un ruolo strategico e di governance complessiva della cybersicurezza

il **Referente della Cybersecurity** (o Responsabile della Sicurezza) si concentra sull'implementazione operativa delle misure

Il **Punto di Contatto NIS 2** è una figura specificamente identificata per la gestione delle comunicazioni e degli adempimenti formali con l'ACN in relazione alla Direttiva NIS 2

Il **RTD** (Responsabile della transizione digitale) Pianifica e coordina le iniziative di digitalizzazione, garantendo coerenza con gli obiettivi di trasformazione digitale, rappresenta l'ente nei rapporti con AgID (Agenzia per l'Italia Digitale), altre PA e fornitori tecnologici per progetti di digitalizzazione

Il **DPO** garantisce la conformità alla normativa sulla protezione dei dati personali, presta consulenza su tutti gli aspetti relativi alla protezione dei dati, è il punto di contatto principale con l'Autorità Garante per la protezione dei dati personali e risponde alle richieste degli interessati in materia di privacy, gestisce le procedure conseguenti ai di data breach

È evidente che la collaborazione sinergica tra queste figure è cruciale

Esempio Pratico

Un ingegnere clinico rileva un malfunzionamento anomalo e generalizzato di diversi dispositivi di diagnostica per immagini. Sospettando un attacco cyber.

Deve immediatamente contattare il Punto di Contatto NIS 2 dell'azienda, che contatta il CISO e il DPO (o contattarli direttamente a seconda

Come queste figure interagiscono in una Azienda Sanitaria

Lo Scenario Integrato

- **Rilevamento:** Un ingegnere clinico nota che un cluster di monitor multiparametrici in terapia intensiva non risponde più correttamente ai comandi o mostra dati errati, e la sua indagine iniziale suggerisce un'anomalia di rete.
- **Segnalazione:** L'ingegnere clinico segnala immediatamente l'anomalia alla struttura IT e al **Referente della Cybersecurity** (o direttamente al CISO se la struttura è piccola), fornendo

Come queste figure interagiscono in una Azienda Sanitaria 2/2

- **Analisi e Decisione:** Il Referente della Cybersecurity e il **CISO**, con il referente IT, analizzano l'incidente per stabilire che è un incidente di cybersicurezza significativo (es. potenziale attacco, impatto sulla continuità del servizio e sulla sicurezza del paziente) che rientra nella NIS 2 e/o compromette dati personali (GDPR).
- **Notifica:** Il **Punto di Contatto NIS 2** designato viene attivato e, sotto la supervisione del CISO, invia la pre-notifica all'ACN entro 24 ore. Se sono coinvolti dati personali, il CISO avvisa il DPO e lo coadiuva nella notifica al Garante.
- **Risposta e Ripristino:** Ingegneri clinici, team IT e CISO lavorano insieme per isolare i dispositivi, contenere l'attacco, ripristinare i servizi in sicurezza *e apprendere dall'incidente*.

Questo esempio mostra l'importanza della collaborazione inter-dipartimentale: IT, Ingegneria Clinica, Privacy, DPO, Direzione Generale che dovrebbe essere sempre notiziata

E le Intelligenze Artific

Entrambe le normative, NIS2 e AI Act, pongono un forte accento sulla **governance** e sulla **responsabilità**

La Direttiva NIS2 affida la responsabilità agli **organi di gestione** per la supervisione della sicurezza informatica

L'AI Act richiede una **governance robusta per i fornitori** di sistemi di AI ad alto rischio.

AI Copilot 2025 13 06

Se le normative sono sinergiche

Anche noi dobbiamo essere sinergici

E ora?

Considerando i vostri dispositivi medici, le infrastrutture che gestite e la situazione generale nella quale si trovano, considerando le risorse ed il grado di libertà che avete a disposizione

decidete le prime tre azioni concrete che pensate di poter intraprendere già da domani per garantire la conformità normativa e la sicurezza dei pazienti

Ricordatevi sempre che la sicurezza dei dati
è come una catena
l'anello più debole che si romperà per primo
è quasi sempre determinato
ttamente dal

fattore umano

Kevin Mitnik

Materiale d'approfondimento

- Il General Data Protection Regulation - Regolamento (UE) 2016/679
- La normativa «privacy» italiana Dlgs 196/2003
- Le linee guida dell'Agenzia per l'Italia Digitale (AgID)
- La Direttiva NIS 2 Direttiva (UE) 2022/2555
- Il Dlgs 138/2024
- Il sito dell'Agenzia per la Cybersecurity Nazionale
- L'IA ACT - Regolamento (UE) 2024/1689

AIIC 2025 CONVEGNO NAZIONALE ASSOCIAZIONE ITALIANA INGEGNERI CLINICI

NAPOLI 14-17 GIUGNO 2025 MOSTRA D'OLTREMARE

AIIC associazione italiana ingegneri clinici

Grazie per l'attenzione!

APIHM Privacy and Information Healthcare Manager Association
Gestione delle informazioni e E-health

graziano.depetris@apihm.it

TECNOLOGIE, SOSTENIBILITÀ, AMBIENTE
Il contributo dell'innovazione alla sanità del futuro