AIIC2023
FORTEZZA DA BASSO
Firenze 10-13 maggio 2023
Convegno Nazionale
Associazione Italiana Ingegneri Clinici
Innovazione e accessibilità:
il governo delle tecnologie sanitarie come sfida sociale
30 AIIC 1993 - 2023

Cybersecurity e dispositivi medici: il punto di vista dell'industria

Fabio Cubeddu
Quality & Regulatory Affairs Specialist
Confindustria Dispositivi Medici

CONFINDUSTRIA
Dispositivi Medici

Cybersecurity e dispositivi medici: il punto di vista dell'industria

L'aumento della **connettività** dei DM alle reti e l'**interoperabilità** che caratterizza le nuove tecnologie espone i dispositivi a un notevole rischio per la sicurezza del paziente.

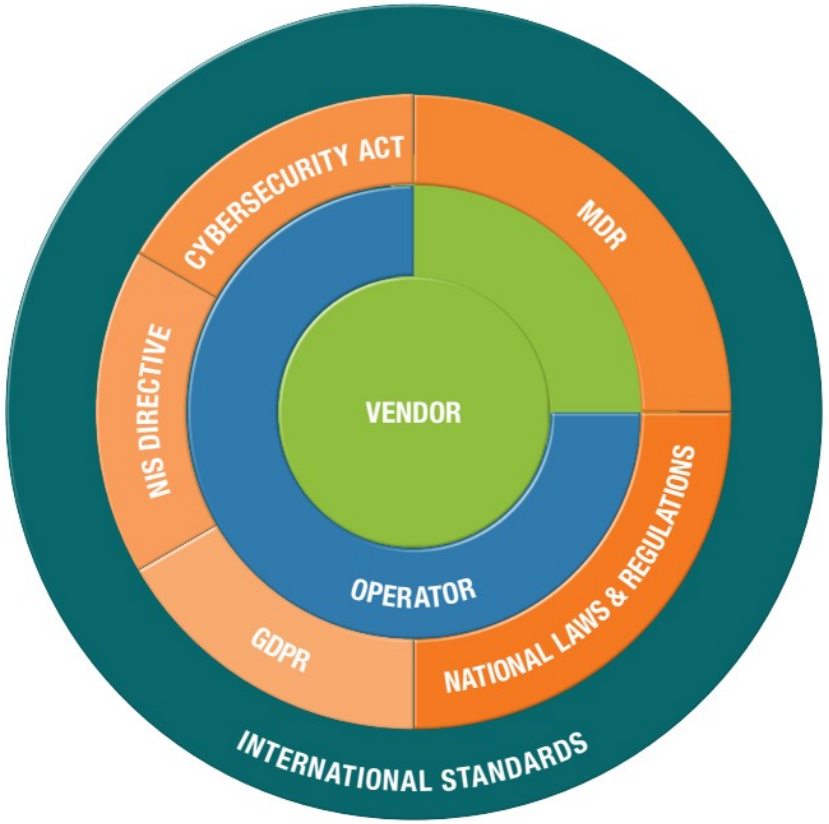
Necessità di **proteggere i dati** da possibili attacchi informatici e la loro compromissione.

Il legislatore ha inserito nei **Regolamenti** aspetti relativi alla protezione e sicurezza dei dati nonché ai requisiti per i software associati ai dispositivi.

Impatto sulla progettazione e fabbricazione dei DM e IVD - **Allegato I (GSPR)**.

Applicazione cogente **per immettere sul mercato europeo** dispositivi medici connessi e interoperabili con altri sistemi e per i software embedded e standalone.

Cybersecurity e dispositivi medici in EU: Framework Normativo



Fonte Cocir: advancing cybersecurity of health and digital technologies

Regolamenti e linee guida di settore:

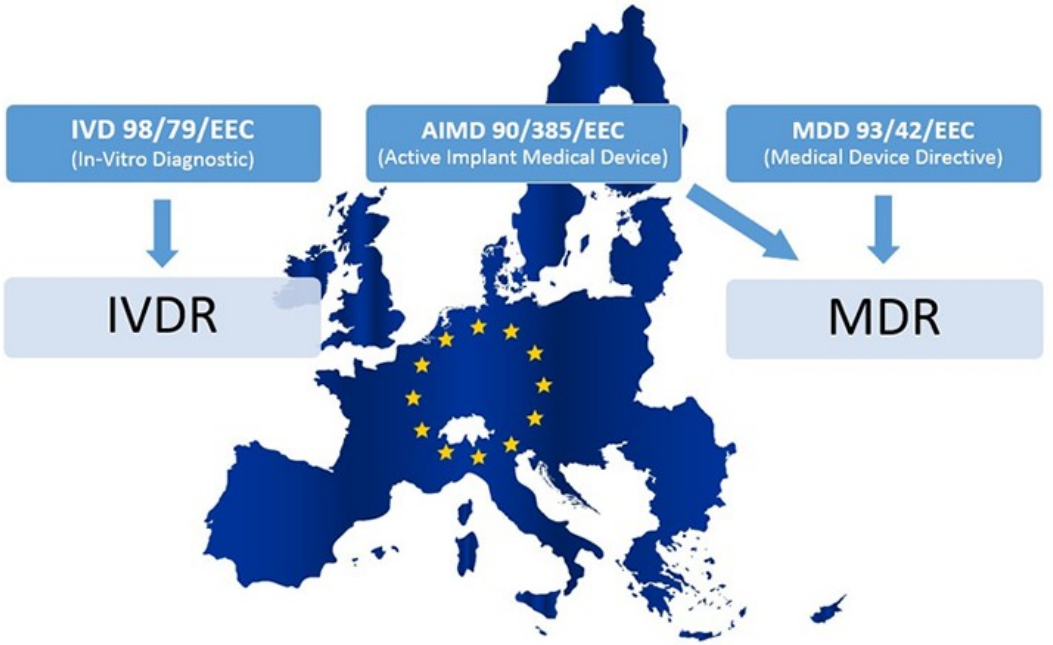
- **Regolamenti 2017/745 (MDR) e 2017/746 (IVDR)**
- **MDCG 2019-16**

Altri standard e regolamenti orizzontali:

- Linee guida IMDRF: ***Principal and practices for Medical Devices Cybersecurity*** e ***Principles and Practices for the Cybersecurity of Legacy Medical Devices***
- Norme tecniche ISO 14971, ISO 13485, ISO 27001, IEC 80001-1, IEC 62304, IEC 82304-1
- **Regolamento per la protezione dei dati - GDPR** - ***privacy by design and default requirements***
- **NIS 2 Directive**
- **EU Cybersecurity act – Regulation (EU) 2019/881**
- **Radio Equipment Directive (RED)**
- **Cyber Resilience Act**
- **AI Act (ongoing)**

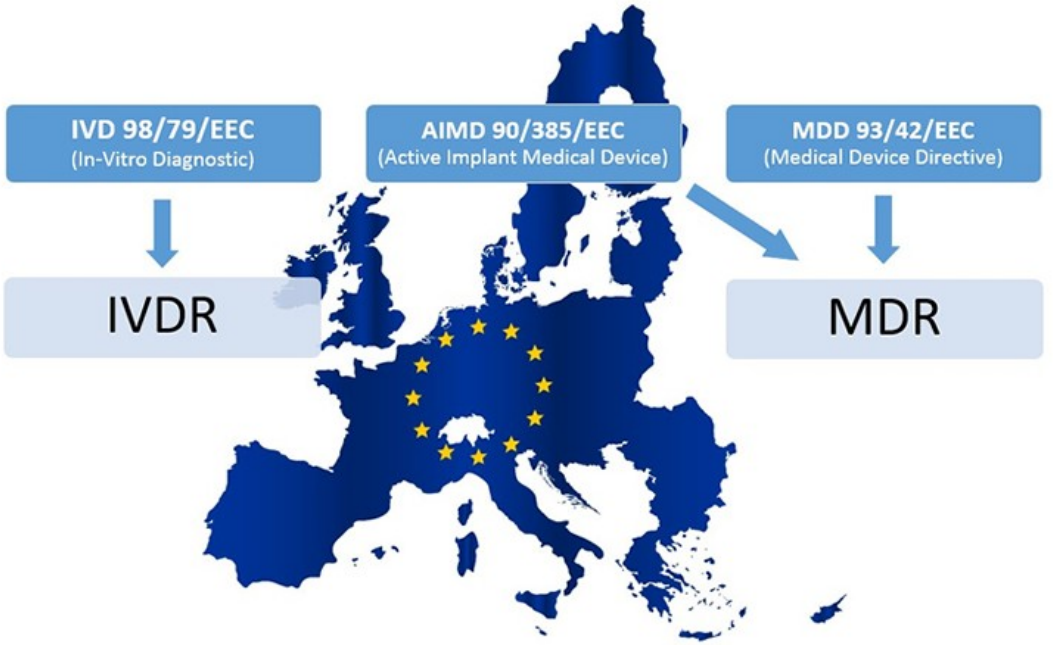
MDR: i punti cardine per l'industria

- **Standard più elevati di qualità, sicurezza ed efficacia** dei dispositivi a beneficio della salute pubblica: il fabbricante deve garantire un sistema di gestione della qualità rigoroso con controlli di progettazione e di produzione completi.
- **Requisiti preclinici e clinici più rigorosi:** il fabbricante deve garantire un'evidenza clinica solida a sostegno del dispositivo. compresi test sulla sicurezza ed efficacia tramite test di laboratorio, indagini cliniche o studi delle prestazioni.
- **Valutazione Rischio-Benefici:** il fabbricante deve condurre una valutazione analitica del rapporto rischi-benefici, per dimostrare che i benefici del prodotto superano i rischi.
- **Classificazione stringente:** il regolamento prevede criteri di classificazione dei dispositivi medici più stringenti basati sul rischio.
- **Sorveglianza post-commercializzazione:** rafforzati i requisiti di sorveglianza post-commercializzazione, con un sistema integrato di registrazione elettronica delle informazioni sui dispositivi (**Eudamed**). Ciò consentirà un monitoraggio più efficace dei dispositivi immessi sul mercato e per le attività di Sorveglianza del mercato da parte delle Autorità competenti.



MDR: i punti cardine per l'industria

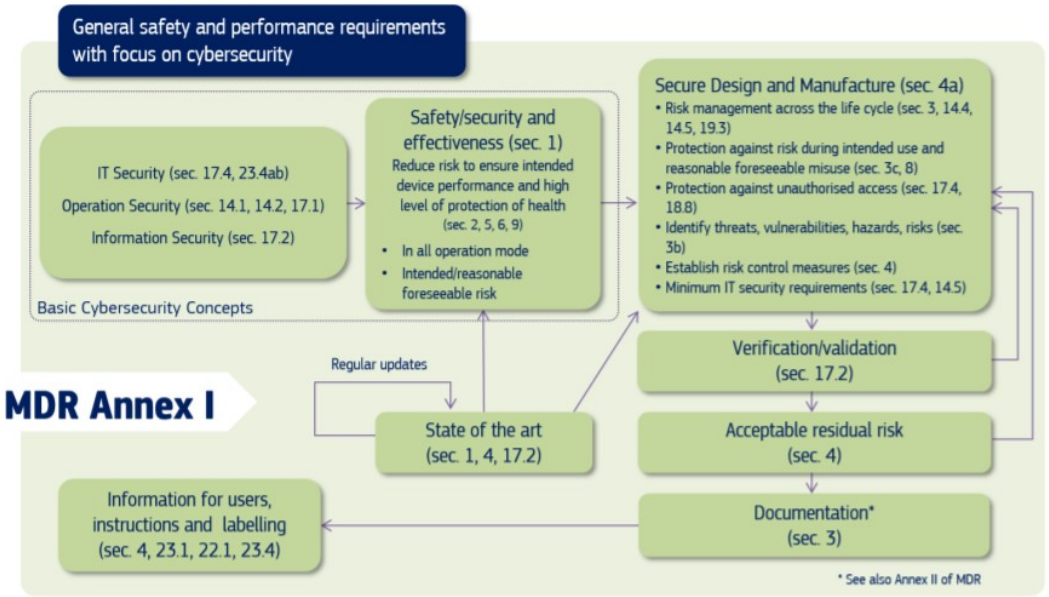
- **Standard più elevati di qualità, sicurezza ed efficacia** dei dispositivi a beneficio della salute pubblica: il fabbricante deve garantire un sistema di gestione della qualità rigoroso con controlli di progettazione e di produzione completi.
- **Requisiti preclinici e clinici più rigorosi:** il fabbricante deve garantire un'evidenza clinica solida a sostegno del dispositivo. compresi test sulla sicurezza ed efficacia tramite test di laboratorio, indagini cliniche o studi delle prestazioni.
- **Valutazione Rischio-Benefici:** il fabbricante deve condurre una valutazione analitica del rapporto rischi-benefici, per dimostrare che i benefici del prodotto superano i rischi.
- **Classificazione stringente:** il regolamento prevede criteri di classificazione dei dispositivi medici più stringenti basati sul rischio.
- **Sorveglianza post-commercializzazione:** rafforzati i requisiti di sorveglianza post-commercializzazione, con un sistema integrato di registrazione elettronica delle informazioni sui dispositivi (**Eudamed**). Ciò consentirà un monitoraggio più efficace dei dispositivi immessi sul mercato e per le attività di Sorveglianza del mercato da parte delle Autorità competenti.



Quali sono i GSPR inerenti alla sicurezza informatica?

Cybersecurity MDR e IVDR

Il punto di partenza è sicuramente la progettazione e la valutazione dei rischi.
→ **GSPR** (all. I, MDR)



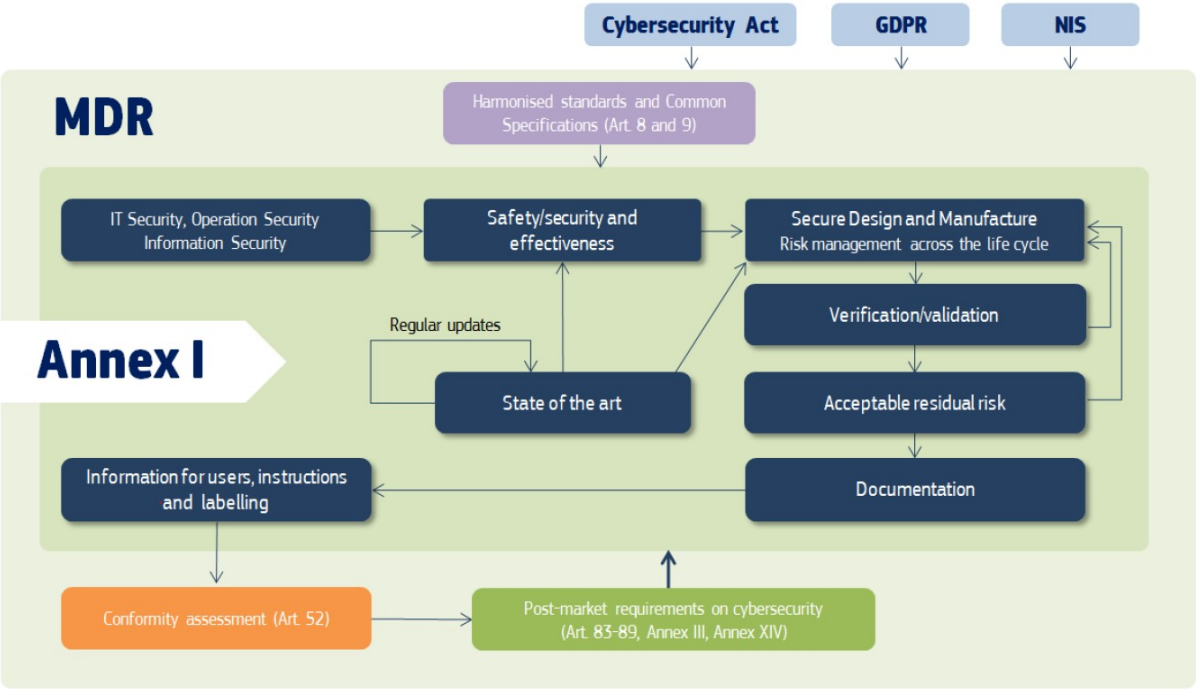
GSPR 17 - Sistemi elettronici programmabili — dispositivi contenenti sistemi elettronici programmabili e software che costituiscono dispositivi a sé stanti.

17.1 I dispositivi contenenti sistemi elettronici programmabili, compresi i software, o i software che costituiscono dispositivi a sé stanti, sono progettati in modo tale da garantire la riproducibilità, l'affidabilità e le prestazioni in linea con la destinazione d'uso per essi prevista. In caso di condizione di primo guasto sono previsti mezzi adeguati per eliminare o ridurre, per quanto possibile, i rischi che ne derivano o il peggioramento delle prestazioni.

17.2 Per i dispositivi contenenti un software o per i software che costituiscono dispositivi a sé stanti, il software è sviluppato e fabbricato conformemente allo stato dell'arte, tenendo conto dei principi del ciclo di vita dello sviluppo, della gestione del rischio, compresa la sicurezza delle informazioni, della verifica e della convalida.

17.4 I fabbricanti indicano requisiti minimi in materia di hardware, caratteristiche delle reti informatiche e **misure di sicurezza informatica, compresa la protezione contro l'accesso non autorizzato**, necessari per far funzionare il software come previsto.

Cybersecurity MDR e IVDR



GSPR 18 - Dispositivi attivi e dispositivi a essi collegati

18.8 I dispositivi sono progettati e fabbricati in modo tale da **proteggerli, per quanto possibile, da accessi non autorizzati** che potrebbero impedire loro di funzionare come previsto.

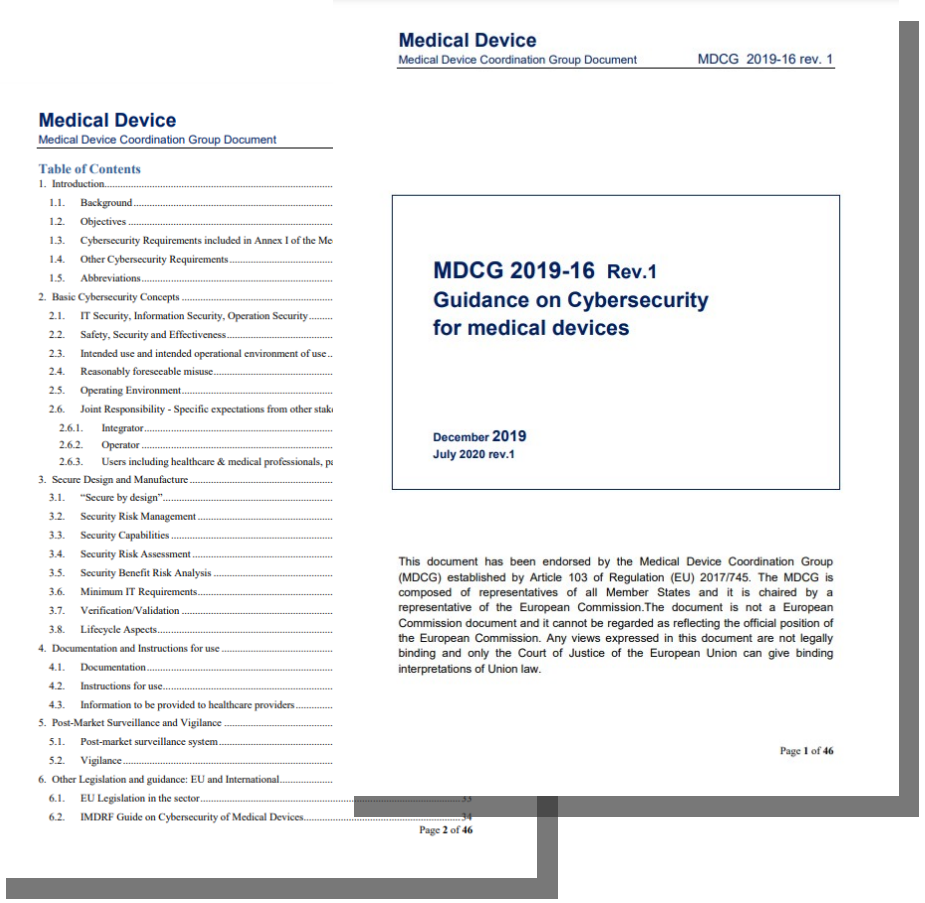
GSPR 23.4 - Informazioni contenute nelle istruzioni per l'uso

a ter) per i dispositivi che contengono sistemi elettronici programmabili, compreso un software, o per i software che costituiscono dispositivi a sé stanti, requisiti minimi in materia di hardware, caratteristiche delle reti informatiche e **misure di sicurezza informatica, compresa la protezione contro l'accesso non autorizzato**, necessari per far funzionare il software come previsto.

GSPR 14 Fabbricazione dei dispositivi e interazione con il loro ambiente

14.2 I dispositivi sono progettati e fabbricati in modo tale da eliminare o ridurre per quanto possibile: [..] d) i rischi associati alla possibile interazione negativa tra il software e l'ambiente tecnologico («ambiente IT») in cui opera e interagisce;

MDCG 2019-16: Guidance on Cybersecurity for MD



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

Medical Device
Medical Device Coordination Group Document

Table of Contents

Page 2 of 46

MDCG 2019-16 Rev.1
Guidance on Cybersecurity for medical devices

December 2019
July 2020 rev.1

This document has been endorsed by the Medical Device Coordination Group (MDCG) established by Article 103 of Regulation (EU) 2017/745. The MDCG is composed of representatives of all Member States and it is chaired by a representative of the European Commission.The document is not a European Commission document and it cannot be regarded as reflecting the official position of the European Commission. Any views expressed in this document are not legally binding and only the Court of Justice of the European Union can give binding interpretations of Union law.

Page 1 of 46

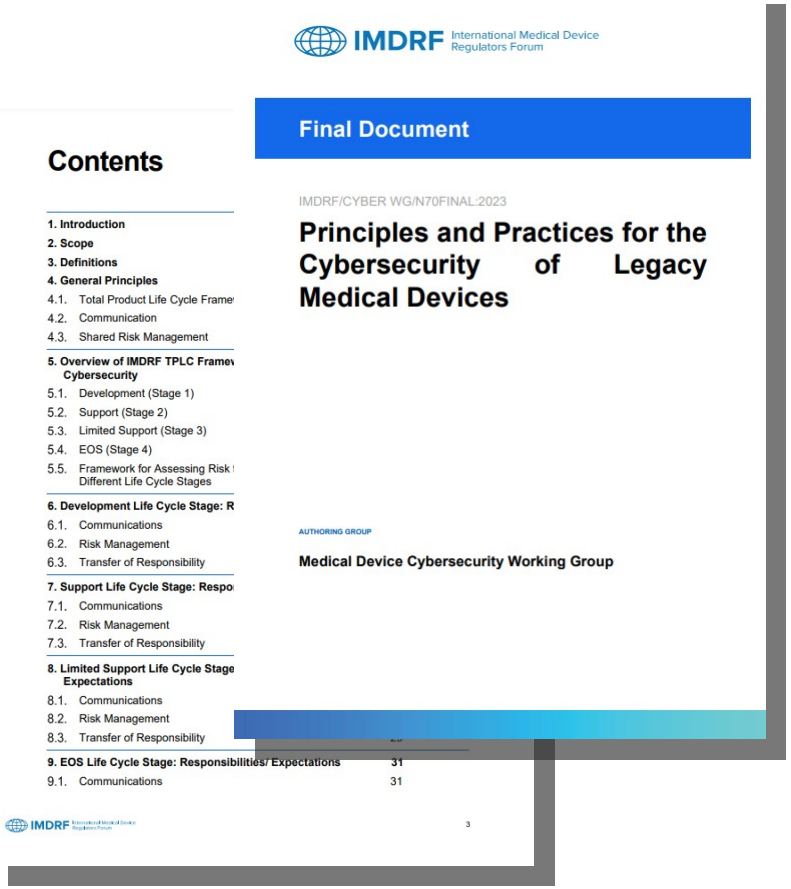
Come l'industria dovrà affrontare i rischi informatici:

1. Inserire la sicurezza informatica direttamente nella fase progettuale e di sviluppo del prodotto.
2. Effettuare una revisione dei rischi, delle minacce e delle vulnerabilità del dispositivo, documentare le scoperte e proattivamente identificare nuove potenziali minacce – **Annex II:** ***Examples of cybersecurity incidents/serious incidents*** della linea guida MDCG 2019-6.
3. Assicurarsi che il software del dispositivo sia accuratamente testato.
4. Esaminare il ciclo di vita dei dati in modo che sia trasparente quali dati sono stati creati e dove e come questi saranno elaborati.
5. Creare e mantenere un registro dei rischi e dei reclami e non conformità.
6. Formazione tecnica del personale qualificato.
7. Includere la sicurezza del ciclo di vita del prodotto prevista in schemi di valutazione dei rischi e di controllo, suscettibile di essere articolata in futuro in capitolati di gara di appalti sanitari.

IMDRF e Cybersecurity

L'International Medical Device Regulators Forum (IMDRF) riunisce autorità di regolamentazione nel settore dei dispositivi medici di tutto il mondo, che si impegnano a promuovere l'allineamento e l'armonizzazione internazionale delle normative vigenti nel settore dei dispositivi medici.

IMDRF e Cybersecurity



IMDRF International Medical Device Regulators Forum

Final Document

IMDRF/CYBER WG/N70FINAL:2023

Principles and Practices for the Cybersecurity of Legacy Medical Devices

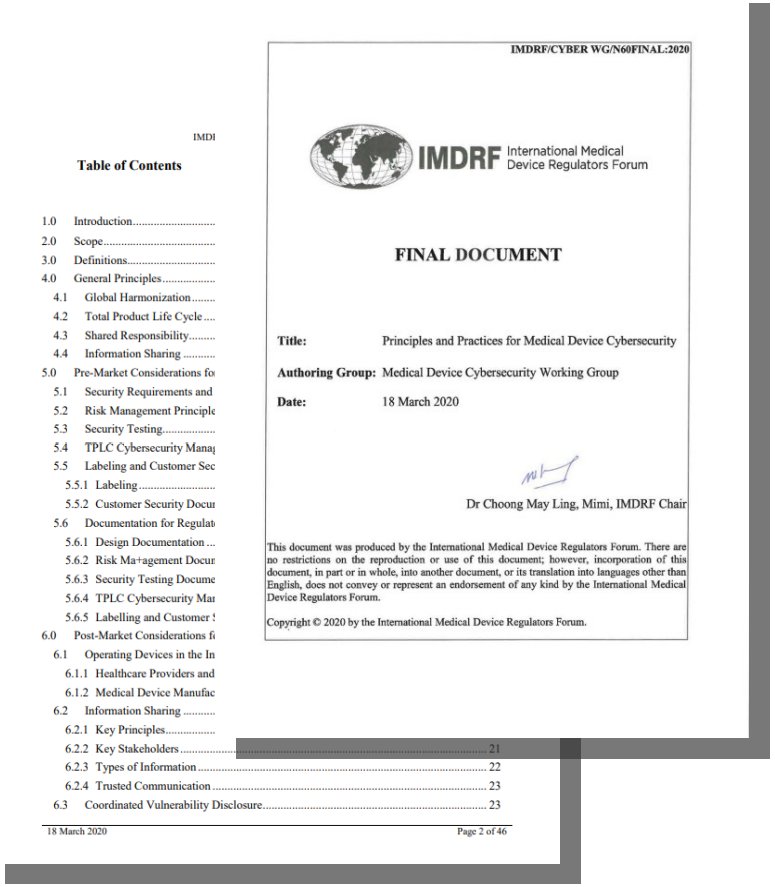
AUTHORING GROUP

Medical Device Cybersecurity Working Group

Contents

IMDRF 3

*"Medical device cybersecurity is a **shared responsibility** and requires participation of **all stakeholders**, including **healthcare providers**. Healthcare providers should consider adopting a risk management process to address the safety, performance, and cybersecurity aspects of medical devices that are connected to their IT infrastructure"*



IMDRF/CYBER WG/N60FINAL:2020

IMDRF International Medical Device Regulators Forum

FINAL DOCUMENT

Title: Principles and Practices for Medical Device Cybersecurity

Authoring Group: Medical Device Cybersecurity Working Group

Date: 18 March 2020

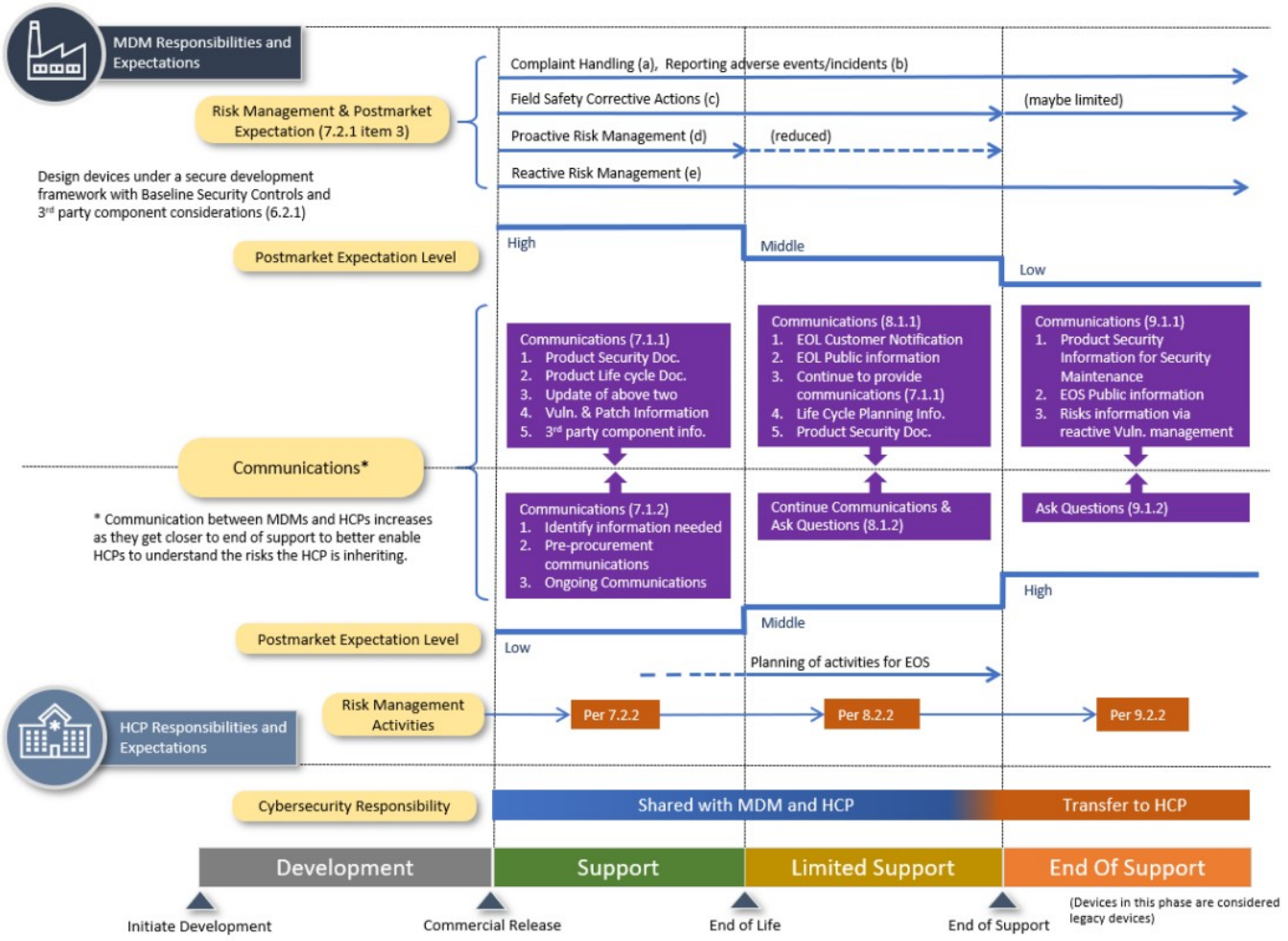
Dr Choong May Ling, Mimi, IMDRF Chair

Table of Contents

18 March 2020 Page 2 of 46

Responsabilità MDM e HCP

- La linea guida IMDRF fornisce una panoramica dettagliata delle **responsabilità e delle aspettative nella gestione della sicurezza informatica dei dispositivi medici** durante il ciclo di vita del prodotto.
- Si parte dalla fase di **sviluppo del prodotto** e man mano che il dispositivo si sposta attraverso le fasi del ciclo di vita, la responsabilità per la gestione della sicurezza informatica passa alla condivisione tra MDM e HCP nella fase di **supporto**, di **supporto limitato** fino alla fase di **fine del supporto**.
- I dispositivi *legacy* descritti nella linea guida presentano rischi di sicurezza informatica che potrebbero essere difficilmente mitigati con la semplice applicazione di patch o aggiornamenti, il che può **rappresentare un pericolo per i pazienti**. La gestione della cybersecurity per i dispositivi medici legacy richiede uno **sforzo congiunto** da parte di tutti gli stakeholder coinvolti.
- Il diagramma fornisce anche una serie di **raccomandazioni** per MDM e HCP in ogni fase del ciclo di vita del DM legacy.

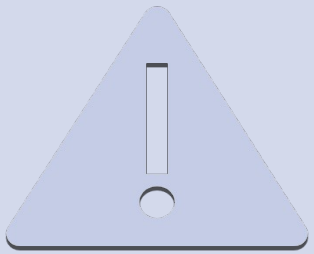


HCP – Misure di controllo

Le misure di controllo rappresentano specifiche misure di controllo del rischio adottate al posto di, o in assenza di, misure di controllo del rischio implementate **come parte di design e progettazione del dispositivo**. Tali misure possono essere permanenti o temporanee e vengono utilizzate quando i dispositivi medici presentano rischi per la sicurezza dei pazienti che non possono essere mitigati con semplici aggiornamenti o patch.
La linea guida IMDRF fornisce alcuni esempi per gli HCP.

Type of control	Compensating risk control measures
Physical access	Restrict physical access to the device to authorized personnel only by placing the device in a restricted area with the appropriate physical entry controls in place. Use of tamper evident seals as appropriate.
Removable media	Restrict the use of removable media such as USB drives by policies in the systems Basic Input Output System/Unified Extended Firmware Interface Forum (BIOS/UEFI), through operating system policies or by physical means.
Network isolation	Isolate the device from the hospital network(s).
Network segregation	Set up a virtual local area network (VLAN) for the device and the other infrastructure/services the device communicates with.
Monitoring	Monitor the device and network for suspicious activity by using an Intrusion Detection System, Intrusion Prevention System or Security Information and Event Management.
Remote access	Remove remote access capabilities from the device.
Firewall	Place the device behind a physical or virtual firewall and only open the ports of the firewall for the network communication that is strictly necessary.
Anti-malware	Install an anti-malware solution on the device, after consultation with the manufacturer. For devices that are isolated from the network (stand-alone), use a solution that does not need definition updates, e.g., an artificial intelligence (AI)-driven anti-malware solution.
Backup and restore	Implement backup and restore procedures to protect against loss of data in case of calamities.

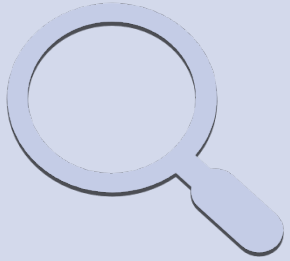
Stato attuale Vs. futuro desiderato



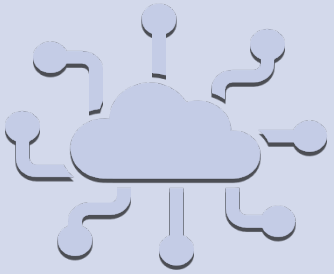
Reattivo/ Incident-driven:

gli eventi vengono affrontati man mano che vengono rilevati.

Protettivo: controlli esterni di compensazione. I controlli esterni ridurranno il numero di eventi.

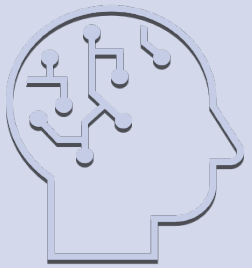


Risk-Based e gestione delle vulnerabilità: Mitigazione basata sulla scoperta e sulla prioritizzazione del rischio.



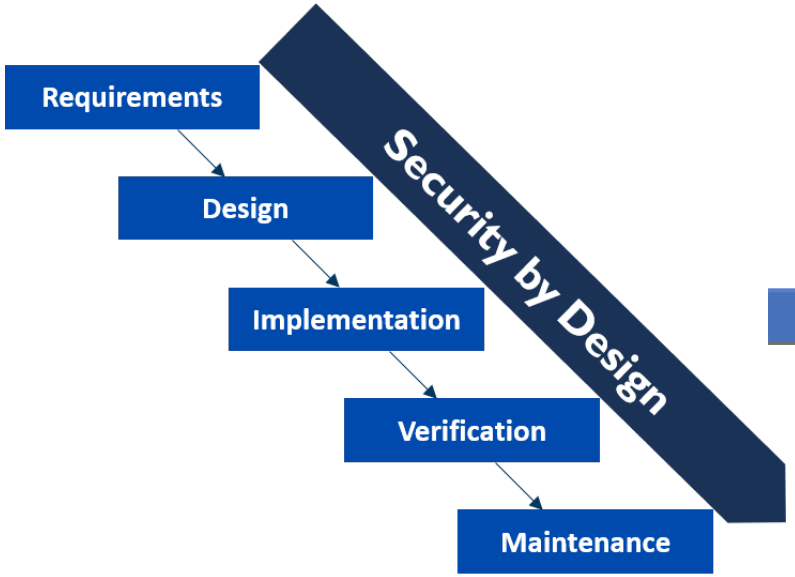
Proattivo, Security by default.

La migliore impostazione di sicurezza possibile al momento dell'immissione sul mercato.



Future-proof: Security by desing. Presunzione di una protezione continua.

Conclusioni: la strategia regolatoria



Punto di partenza: considerare gli aspetti di cybersecurity fin dalle prime fasi di sviluppo del DM (vedi All. I – GSPR + norme tecniche ISO 14971, ISO 27001, IEC 80001-1, IEC 62304, IEC 82304-1).

Uso sicuro del DM, fornendo ai pazienti e/o agli utilizzatori tutte le informazioni necessarie, comprese le buone pratiche di "**cyber igiene**".

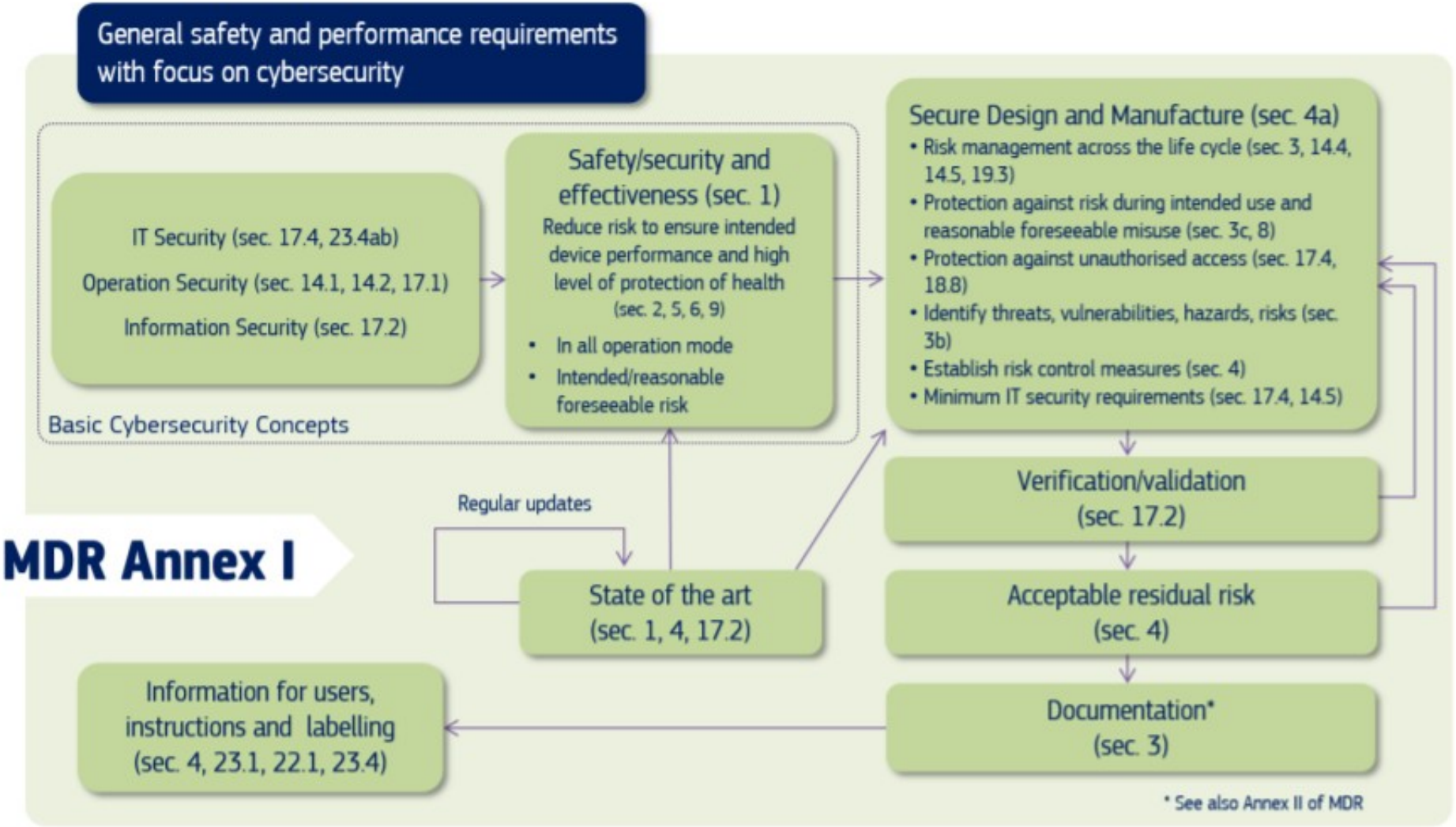
Collaborazione con clienti, operatori sanitari, pazienti, ricercatori sulla sicurezza e altri, verso l'obiettivo della «**sicurezza attraverso la partnership».** Le aziende possono emettere regolarmente divulgazioni di sicurezza coordinate volontarie, al fine di condividere informazioni con i clienti sulle potenziali vulnerabilità che identificano o di cui vengono a conoscenza e su come i clienti possono proteggere se stessi e i loro pazienti.

GRAZIE!

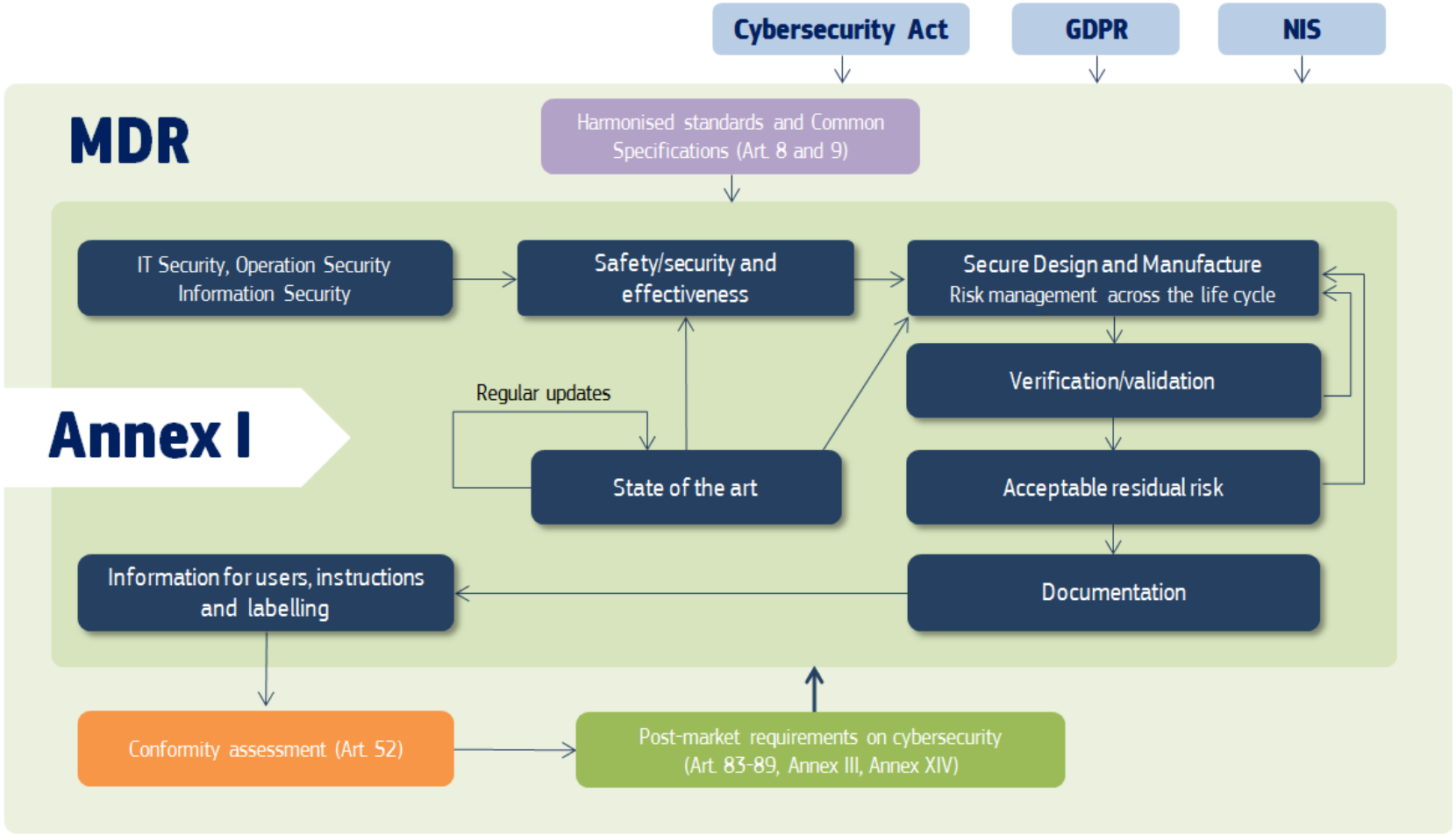
Domande?

cubeddu@confindustriadm.it
quality.regulatory@confindustriadm.it

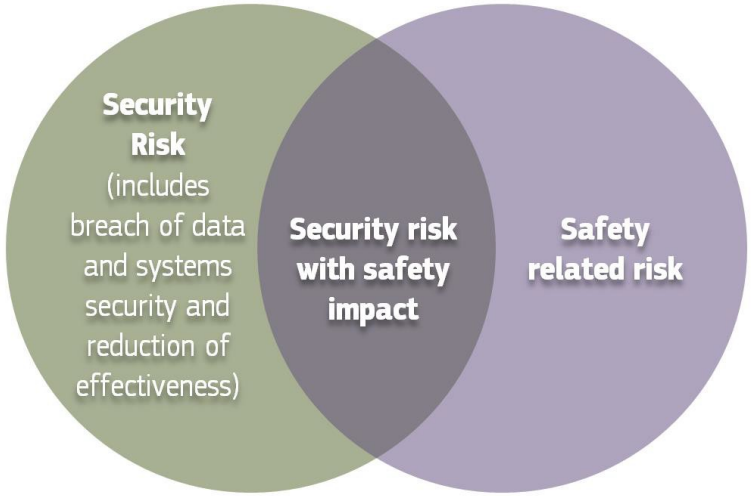
Cybersecurity MDR e IVDR



Cybersecurity MDR e IVDR



Cybersecurity MDCG



[…] there is a need to consider the relationship between "safety and security" as they relate to risk. As illustrated below in Figure 3 patients' safety may be compromised due to "security issues" which may have "safety impacts".