Elevare la sicurezza dei dispositivi medici: l'importanza della cybersecurity nella valutazione del rischio della sperimentazione clinica

Ministero della Salute

Lucia Rita Quitadamo
Ufficio 6-Direzione generale dei dispositivi medici e del farmaco

Regolamenti e linee guida

REGOLAMENTO UE 2017/745

5.5.2017 IT Gazzetta ufficiale dell'Unione europea L 117/1

I

(Atti legislativi)

REGOLAMENTI

REGOLAMENTO (UE) 2017/745 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

del 5 aprile 2017

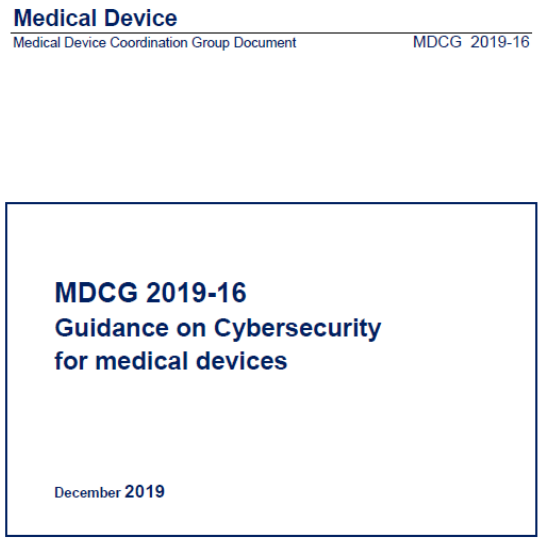
relativo ai dispositivi medici, che modifica la direttiva 2001/83/CE, il regolamento (CE) n. 178/2002 e il regolamento (CE) n. 1223/2009 e che abroga le direttive 90/385/CEE e 93/42/CEE del Consiglio

(Testo rilevante ai fini del SEE)

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea, in particolare l'articolo 114 e l'articolo 168, paragrafo 4, lettera c),

MEDICAL DEVICE COORDINATION GROUP



Medical Device

Medical Device Coordination Group Document MDCG 2019-16

MDCG 2019-16

Guidance on Cybersecurity for medical devices

December 2019

INTERNATIONAL MEDICAL DEVICE REGULATORS FORUM

IMDRF International Medical Device Regulators Forum

DRAFT DOCUMENT

International Medical Device Regulators Forum

Title: Principles and Practices for Medical Device Cybersecurity

Authoring Group: Medical Device Cybersecurity Working Group

Date: October 1, 2019

Obblighi generali dei Fabbricanti di dispositivi medici (Art. 10 Regolamento)

1) Istituire, documentare, applicare, mantenere, aggiornare e migliorare costantemente un **sistema di gestione della qualità** che garantisca la conformità al Regolamento nella maniera più efficace e in modo proporzionato alla classe di rischio e alla tipologia di dispositivo.

> *Il sistema di gestione della qualità riguarda tutte le parti e gli elementi dell'organizzazione del fabbricante che si occupano della qualità di processi, procedure e dispositivi. Esso disciplina la struttura, le competenze, le procedure, i processi e le risorse gestionali richiesti per attuare i principi e le azioni necessari a conseguire il rispetto delle disposizioni del Regolamento*

2) Istituire, documentare, attuare e mantenere un **sistema per la gestione del rischio** per individuare e analizzare i pericoli noti e prevedibili associati a ciascun dispositivo.

Obblighi generali dei Fabbricanti di dispositivi medici (Art. 10 Regolamento)

3) Effettuare una **valutazione clinica** (nel rispetto dei requisiti di cui all'articolo 61 e all'allegato XIV) ivi compreso un *post-market clinical follow-up*.

Valutazione clinica: un processo sistematico e programmato atto a generare, raccogliere, analizzare e valutare in maniera continuativa i dati clinici relativi a un dispositivo per verificarne la sicurezza e la prestazione, benefici clinici compresi, quando è utilizzato come previsto dal fabbricante

Sicurezza: assenza di rischi inaccettabili

Prestazione clinica: la capacità di un dispositivo, dovuta a effetti medici, diretti o indiretti, derivanti dalle sue caratteristiche tecniche o funzionali, ivi comprese diagnostiche, di ottenere la destinazione d'uso dichiarata dal fabbricante, procurando in tal modo un beneficio clinico per i pazienti, quando è utilizzato come previsto dal fabbricante

Beneficio clinico:

- impatto positivo di un dispositivo sulla salute di una persona, definito in termini di esito clinico significativo, misurabile e rilevante per il paziente
- impatto positivo sulla gestione del paziente o sulla salute pubblica

Post-market clinical follow-up (PMCF): un processo continuo che aggiorna la **valutazione clinica** ed è trattato nel piano di sorveglianza post-commercializzazione del fabbricante. Nel realizzare il PMCF, **il fabbricante raccoglie e valuta in modo proattivo i dati clinici relativi all'uso negli o sugli esseri umani di un dispositivo che reca la marcatura CE ed è immesso sul mercato o messo in servizio nei limiti della destinazione d'uso** indicata nel procedimento di valutazione della conformità pertinente, allo scopo di confermare la sicurezza e le prestazioni per tutta la vita prevista del dispositivo, di assicurare l'immutata accettabilità dei rischi identificati e di rilevare rischi emergenti sulla base di elementi fattuali.

Valutazione clinica

art 61. Regolamento

La valutazione clinica segue una **procedura definita e metodologicamente valida** fondata su:

- **un'analisi critica della letteratura scientifica** - a condizione che sia dimostrato che il dispositivo oggetto della valutazione clinica per la destinazione d'uso è equivalente e che i dati dimostrino adeguatamente la conformità ai pertinenti requisiti generali di sicurezza e prestazione

- **un'analisi critica dei risultati** di tutte **le indagini cliniche** disponibili, tenendo in debita considerazione il fatto che le indagini siano state effettuate secondo il nuovo Regolamento

- un **esame delle eventuali opzioni di trattamento** alternativo attualmente disponibili per lo stesso scopo

Ipotesi di studio
Disegno studio
Dimensione campione
Controllo bias
Follow-up
Statistica
Conclusioni
…….
Applicazione Regolamento

Comparazione dei risultati con i trattamenti disponibili

Indagini cliniche

Qualsiasi indagine sistematica in uno o più soggetti umani, volta a **valutare la sicurezza o le prestazioni** di un dispositivo.

- Indagini cliniche svolte con dispositivi non marcati CE pianificate al fine della valutazione della conformità del dispositivo medico oggetto di indagine ai requisiti generali del Regolamento (art. 62, comma 1, cosiddette pre-market)
- Indagini cliniche PMCF - pianificate al fine della conferma della conformità del dispositivo ai requisiti generali del Regolamento (art. 74 , Allegato XIV -B)
- Indagini cliniche pianificate per fini diversi (art. 82)

Valutazione da parte degli Stati Membri (art. 71)

3. Gli Stati membri valutano se l'indagine clinica è progettata in modo tale che i potenziali rischi rimanenti per i soggetti o per terzi, dopo la minimizzazione del rischio, siano giustificabili tenuto conto dei benefici clinici previsti. Tenendo in considerazione le SC o le norme armonizzate applicabili, essi esaminano in particolare:

a) la dimostrazione della conformità del o dei dispositivi oggetto dell'indagine ai requisiti generali di sicurezza e prestazione applicabili, a eccezione degli aspetti che formano oggetto dell'indagine clinica e, per questi ultimi, se sono state prese tutte le precauzioni per proteggere la salute e la sicurezza dei soggetti. Esse includono, se del caso, la garanzia dello svolgimento di test di sicurezza tecnica e biologica e di una valutazione preclinica;

b) se le soluzioni di minimizzazione del rischio impiegate dallo sponsor sono descritte nelle norme armonizzate e, nei casi in cui lo sponsor non utilizza norme armonizzate, se le soluzioni di minimizzazione del rischio forniscono un livello di protezione equivalente a quello fornito dalle norme armonizzate;

c) se le misure previste per l'installazione, la messa in servizio e la manutenzione sicure del dispositivo oggetto di indagine sono adeguate;

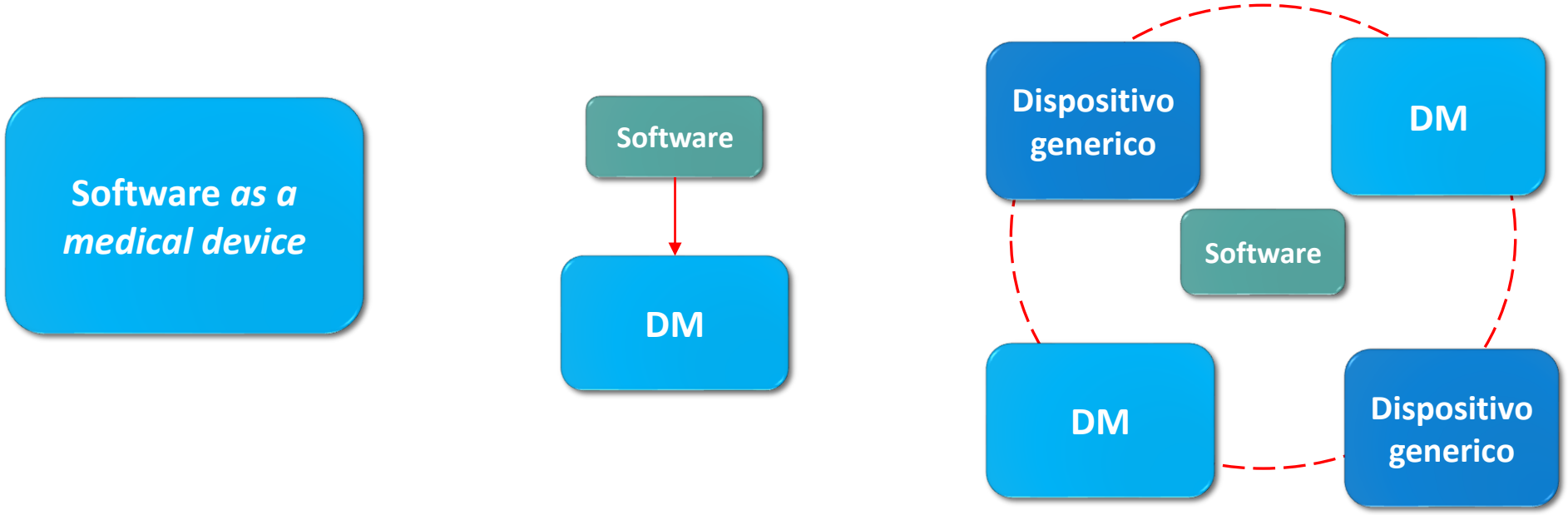
d) l'affidabilità e la solidità dei dati ottenuti dall'indagine clinica, tenendo conto degli approcci statistici, della progettazione dell'indagine e degli aspetti metodologici, compresi le dimensioni del campione, il comparatore e gli *endpoint*;

e) se sono rispettati i requisiti dell'allegato XV;

f) per i dispositivi per uso sterile, il test della convalida delle procedure di sterilizzazione utilizzate dal fabbricante o le informazioni sulle procedure di ricondizionamento e sterilizzazione che devono essere svolte dal sito di indagine;

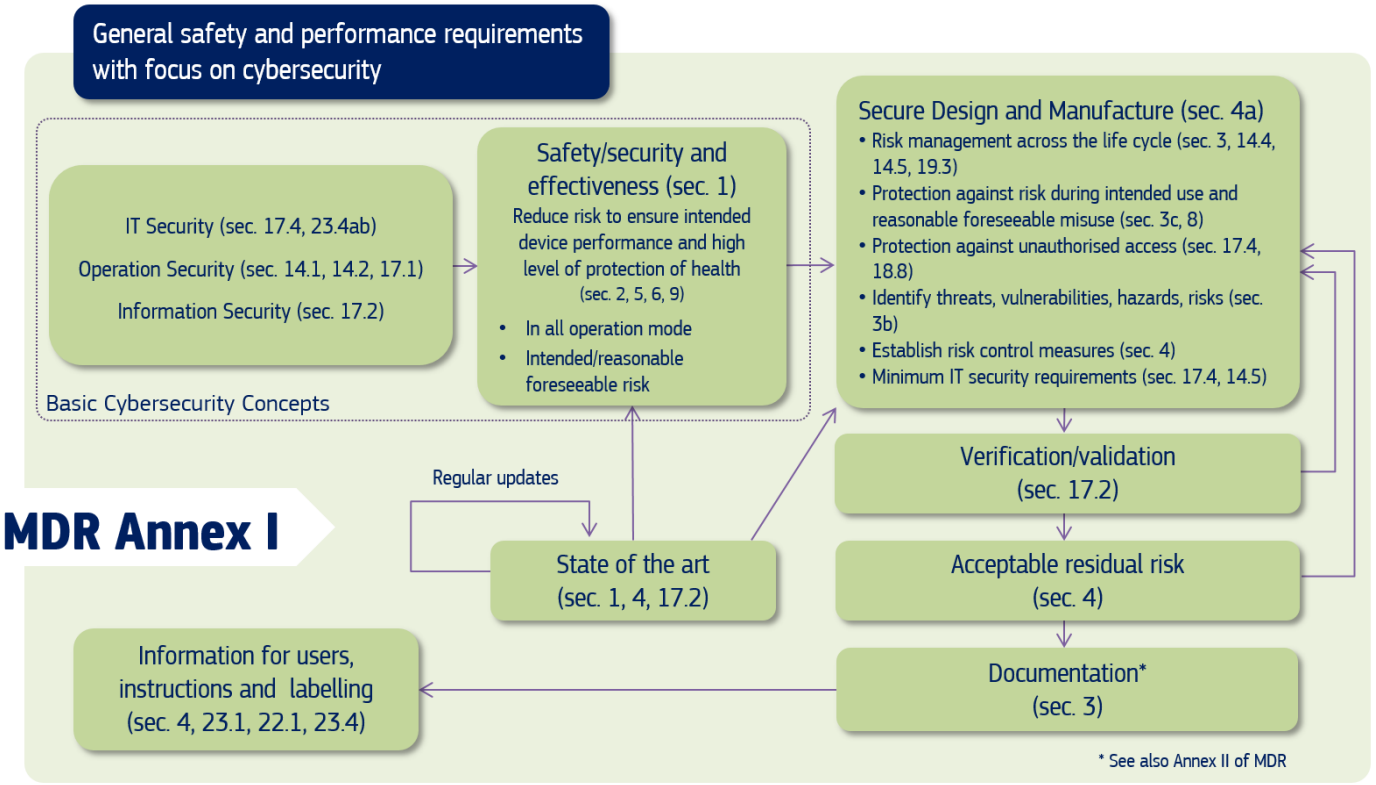
g) la dimostrazione della sicurezza, qualità e utilità dei componenti di origine animale o umana o di sostanze che possono essere considerate medicinali conformemente alla direttiva 2001/83/CE.

Valutazione di dispositivi che coinvolgono software



- Compito del Fabbricante è quello di definire la destinazione d'uso e le funzionalità dei componenti che compongono il dispositivo oggetto di indagine
- Inquadramento regolatorio ed analisi dei rischi diventano complesse quando sono presenti software e diversi dispositivi connessi.

Requisiti generali di sicurezza prestazione connessi alla cybersecurity (Allegato I)



Main topic	Section number MDR Annex I
Device performance	1
Risk reduction	2
Risk management system	3
Risk control measures	4
Minimisation of foreseeable risks, and any undesirable side-effects	8
Combination/connection of devices/systems	14.1
Interaction between software and the IT environment	14.2.d
Interoperability and compatibility with other devices or products	14.5
Repeatability, reliability and performance	17.1
Development and manufacture in accordance with the state of the art taking into account the principles of development life cycle, risk management, including information security, verification and validation	17.2
Minimum IT requirements	17.4
Unauthorised access	18.8
Lay persons	22.1
Residual risks (information supplied by the manufacturer)	23.1 g
Warnings or precautions (information on the label)	23.2 m
Residual risks, contra-indications and any undesirable side-effects, (information in the instructions for use)	23.4 g
Minimum IT requirements (information in the instructions for use)	23.4.ab

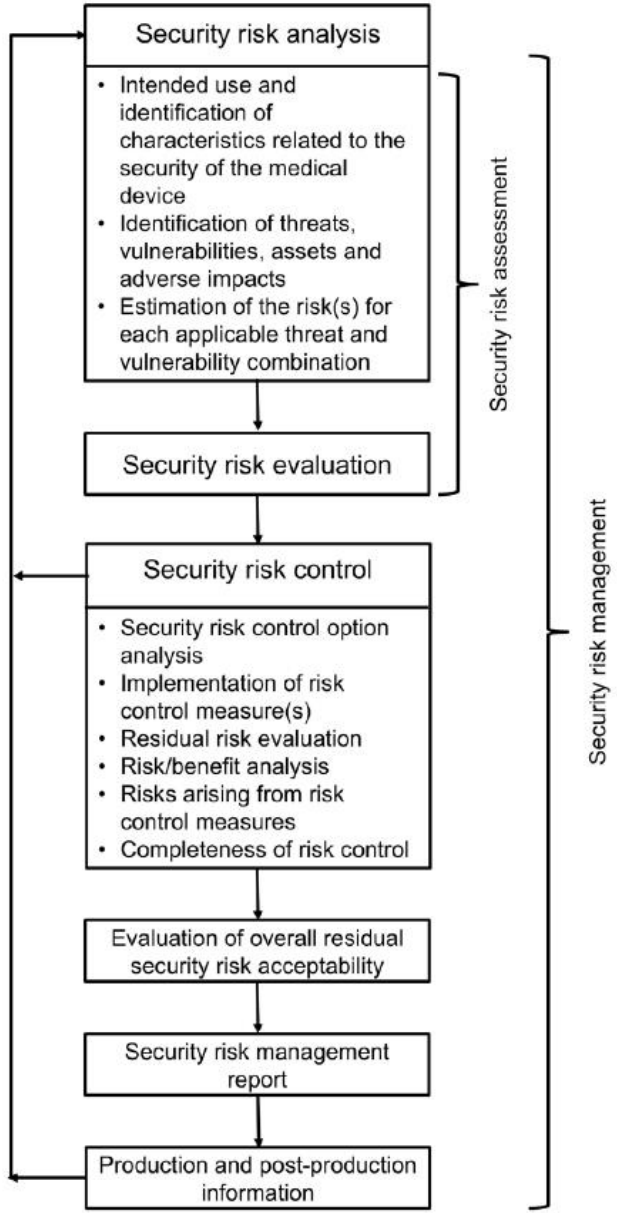
Analisi dei rischi

Un rischio di cybesecurity che ha un impatto sulla sicurezza e le performance dei dispositivi, può portare a errori nella diagnosi o nella terapia per un paziente

Il Fabbricante deve:

- Identificare le vulnerabilità da cybersecurity
- Stimare e valutare i rischi associati
- Mitigare i rischi ad un livello accettabile
- Monitorare l'efficacia delle misure di controllo del rischio

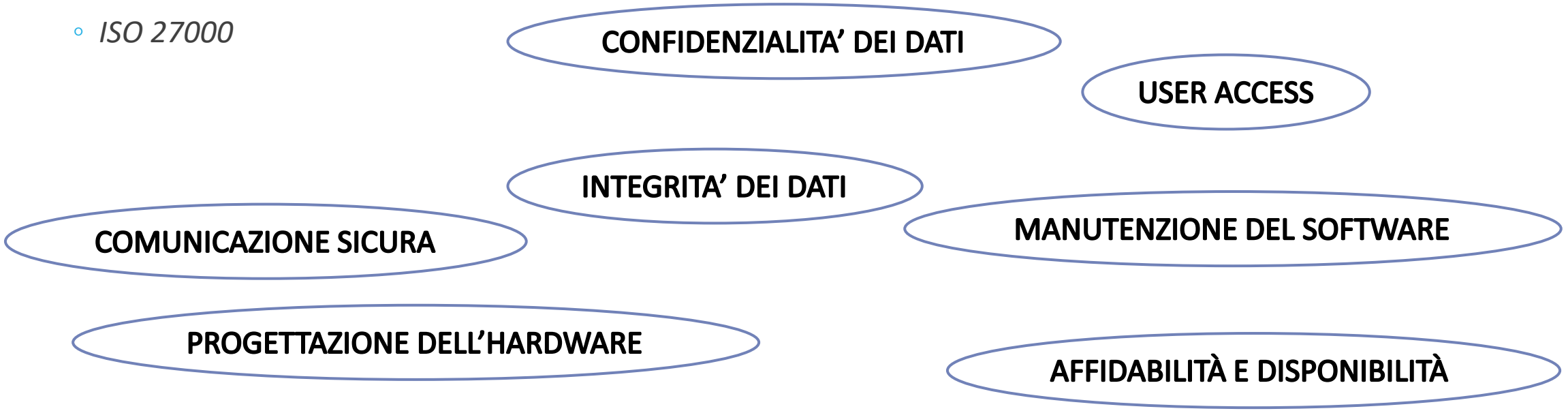
Standard ISO 14971:2019 - Medical devices — Application of risk management to medical devices



Considerazioni pre-market sulla cybersecurity

1) REQUISITI DI SICUREZZA E PROGETTAZIONE DELL'ARCHITETTURA

- *IEC 62304: Software Lifecycle*
- *IEC 60601-1-requisiti per PEMS (programmable electrical medical system)*
- *IEC TR 80001-2-2*
- *IEC 80001-2-8*
- *ISO 27000*



Considerazioni pre-market sulla cybersecurity

2) SECURITY TESTING

La convalida della fase di progettazione di un dispositivo medico richiede **test di sicurezza**. I test devono prendere in considerazione il **contesto di utilizzo** del dispositivo e il relativo ambiente di distribuzione. Si raccomanda l'applicazione di tecniche di verifica del software per ridurre al minimo il rischio di anomalie e garantire che il software sia conforme alle specifiche:

- Eseguire ricerche mirate su componenti/moduli software per **individuare vulnerabilità note o debolezze del software**. Ad esempio, i test di sicurezza possono includere: analisi del codice statico, analisi dinamica, test di robustezza, scansione delle vulnerabilità, analisi della composizione del software.
- **Condurre analisi tecniche di sicurezza (e.g. test di penetrazione),** per identificare vulnerabilità sconosciute e per condurre controlli per vulnerabilità sconosciute; o verificare la presenza di punti di ingresso alternativi, ad esempio leggendo file nascosti, file di configurazione, flussi di dati o registri hardware.
- **Completare una valutazione della vulnerabilità,** ad esempio un'analisi dell'impatto della vulnerabilità su altri prodotti interni (ad esempio l'analisi delle varianti); l'identificazione delle contromisure e la correzione o la mitigazione della vulnerabilità.

Considerazioni pre-market sulla cybersecurity

3) STRATEGIA DI GESTIONE POST-MARKET

Prima dell'ingresso sul mercato dovrebbe essere elaborato un **piano per il monitoraggio continuo** delle risposte alle minacce emergenti relativamente alla cybersicurezza. Questo piano dovrebbe essere applicato per tutto il ciclo di vita del dispositivo. Gli elementi da considerare come parte di questo piano, sviluppati prima dell'ingresso sul mercato, dovrebbero includere:

- Vigilanza post-commercializzazione: un piano per monitorare e identificare in modo proattivo le vulnerabilità della sicurezza informatica scoperte di recente, valutarne le minacce e rispondere.
- Divulgazione delle vulnerabilità: un processo formalizzato per la raccolta di informazioni dai cercatori di vulnerabilità, lo sviluppo di strategie di mitigazione e correzione e la divulgazione dell'esistenza di vulnerabilità
- Patch e aggiornamenti: un piano che delinea come verrà aggiornato il software per mantenere la sicurezza e le prestazioni del dispositivo regolarmente o in risposta a una vulnerabilità identificata.
- Ripristino: un piano di ripristino per il produttore, l'utente o entrambi per ripristinare il dispositivo alle normali condizioni operative a seguito di un incidente di sicurezza informatica.
- Condivisione delle informazioni: partecipazione a organizzazioni di analisi della condivisione delle informazioni o centri di condivisione e analisi delle informazioni che promuovono la comunicazione e la condivisione di informazioni aggiornate sulle minacce alla sicurezza e le vulnerabilità

Considerazioni pre-market sulla cybersecurity

4) ISTRUZIONI PER L'USO E DOCUMENTAZIONE PER L'UTENTE/HEALTHCARE PROVIDERS RELATIVA ALLA CYBERSECURITY

- Istruzioni relative ai controlli di sicurezza informatica consigliati e appropriati per l'ambiente di utilizzo previsto (ad es. software antivirus, uso di un firewall).
- Descrizione delle funzionalità e delle procedure di backup e ripristino per ripristinare le configurazioni.
- Linee guida specifiche per gli utenti in merito ai requisiti dell'infrastruttura di supporto in modo che il dispositivo possa funzionare come previsto.
- Descrizione di come il dispositivo può essere protetto utilizzando una configurazione sicura. Le configurazioni sicure possono includere protezioni degli endpoint come anti-malware, regole firewall/firewall, whitelisting, parametri degli eventi di sicurezza, parametri di registrazione, rilevamento della sicurezza fisica.
- Un elenco di porte di rete e altre interfacce che dovrebbero ricevere e/o inviare dati e una descrizione della funzionalità della porta e se le porte sono in entrata o in uscita (si noti che le porte inutilizzate devono essere disabilitate).
- Istruzioni tecniche per consentire l'implementazione e la manutenzione sicure della rete (connessa) e istruzioni per gli utenti su come rispondere al rilevamento di una vulnerabilità o di un incidente di sicurezza informatica.
- Una descrizione di come il dispositivo o i sistemi di supporto avviseranno l'utente quando vengono rilevate condizioni anomale. I tipi di eventi di sicurezza potrebbero essere modifiche alla configurazione, anomalie di rete, tentativi di accesso, traffico anomalo (ad esempio, invio di richieste a entità sconosciute).
- Una descrizione dei metodi per la conservazione e il ripristino della configurazione del dispositivo da parte di un utente privilegiato autenticato.
- I rischi dell'utilizzo del dispositivo medico al di fuori dell'ambiente di utilizzo previsto.
- Una descrizione delle procedure sistematiche per gli utenti autorizzati a scaricare e installare gli aggiornamenti dal produttore.

Considerazioni post-market sulla cybersecurity

SISTEMA DI SORVEGLIANZA POST-MARKET (art.83)

- aggiornare la valutazione dei rischi e dei benefici e migliorare la gestione del rischio;
- aggiornare le informazioni di progettazione e fabbricazione, le istruzioni per l'uso e l'etichettatura;
- aggiornare la valutazione clinica;
- aggiornare la sintesi relativa alla sicurezza e alla prestazione clinica;
- identificare le esigenze di azioni preventive, correttive e correttive di sicurezza;
- individuare le possibilità di migliorare l'utilizzabilità, le prestazioni e la sicurezza del dispositivo-,
- …

VIGILANZA (art. 87)

I fabbricanti segnalano alle pertinenti autorità competenti :

a) qualsiasi **incidente grave** relativo a dispositivi messi a disposizione sul mercato dell'Unione, eccetto gli effetti collaterali attesi che sono chiaramente documentati nelle informazioni sul prodotto e quantificati nella documentazione tecnica e che sono oggetto di relazioni sulle tendenze ai sensi dell'articolo 88;

b) qualsiasi **azione correttiva di sicurezza** relativa a dispositivi messi a disposizione sul mercato dell'Unione, incluse le azioni correttive di sicurezza intraprese in un paese terzo in relazione a un dispositivo messo legittimamente a disposizione anche sul mercato dell'Unione se l'azione correttiva in questione non è causata solo dal dispositivo messo a disposizione nel paese terzo.

Esempi di incidenti connessi alla cybersecurity

POMPA DI INFUSIONE CON CONTROLLO REMOTO	**Il paziente può riconfigurare il dispositivo**	**Pompa di infusione infonde più o meno insulina rispetto a quanto prescritto da un utente autorizzato.**
PACEMAKER	**Un utente non autorizzato è in grado di affaticare il dispositivo sovraccaricando il dispositivo di richieste.**	**Potrebbe verificarsi un esaurimento prematuro della batteria.**
DISPOSITIVI MEDICI CON WINDOWS	**Il malware diffuso in rete crittografa il contenuto del disco rigido del sistema**	**Dispositivo inutilizzabile**
MACCHINA RAGGI X	**Sistema attaccato e compromesso tramite interfacce di rete/terze parti legacy vulnerabili che si integrano con il dispositivo medico.**	**Ritardo nella diagnosi e nei trattamenti**

Considerazioni post-market sulla cybersecurity: responsabilità condivise

Uso dei dispositivi nell'ambiente di utilizzo previsto

Healthcare providers

- ✓ Gestione del rischio per garantire la sicurezza e l'efficacia di dispositivi medici integrati nell'infrastruttura IT;
- ✓ Training di tutti gli utenti

Fabbricanti

Condivisione delle informazioni

-vulnerabilità dei prodotti
-vulnerabilità dei componenti utilizzati in altri prodotti
-apparecchiature informatiche che possono avere un impatto sulla sicurezza dei dispositivi medici
-attacchi, potenzialità e sviluppo di exploit
-conferma di incidenti
-disponibilità di patch o alternative più sicure

Autorità competenti
Healthcare organizations
Utilizzatori
Fabbricanti
Distributori

Altre legislazioni EU

DIRETTIVA 2022/2555 sull'adozione di misure volte a **garantire un elevato livello di cybersecurity nell'Unione (NIS2).**

Obiettivi:

- obblighi per gli Stati nazionali di adottare strategie sulla **cyber sicurezza**, istituendo **autorità nazionali competenti**, **autorità di gestione** delle crisi informatiche, **punti di contatto** unici in materia di sicurezza (punti di contatto unici) e team di risposta agli incidenti di sicurezza informatica (CSIRT);
- **misure sulla gestione dei rischi di cybersecurity** e obblighi di segnalazione;
- **obblighi di condivisione delle informazioni** sulla cybersecurity;
- **obblighi di vigilanza.**

REGOLAMENTO 2016/679 GENERALE SULLA PROTEZIONE DEI DATI

1. Stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati.
2. Protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali.
3. La libera circolazione dei dati personali nell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.

Standards

- **EN ISO 14971** Risk Management (Product)
- **EN 62304** Software Lifecycle
- **EN ISO 31000** Risk Management (Organisation) or particular standards under ISO 31xxx.
- **EN ISO/IEC 27000** Information technology — Security techniques — Information security management systems (ISMS) — Overview and vocabulary
- **EN ISO/IEC 27001** Information Technology – Security techniques – Information Security management Systems – Requirements.
- **EN ISO/IEC 60601-1-x**
- **IEC 82304-1** Health Software Part 1: General requirements for Product Safety
- **ISO/IEC 80001-1** Application of Risk Management for IT networks Incorporating Medical Devices
- **ISO/IEC 80001-5-1** Application of Risk Management for IT networks incorporating medical device – Safety, effectiveness and security in the implementation and use of connected medical devices or connected health software – Part 5-1: Activities in the product life-cycle.
- **IEC/TR 80001-2-2** Application of Risk Management for IT networks Incorporating Medical Devices Part 2-2: Guidance for the Disclosure and Communication of MS Security Needs, Risks and Controls
- **IEC/TR 80001-2-8** Application of risk management for IT-networks incorporating medical devices – Part 2-8: Application guidance – Guidance on standards for establishing the security capabilities identified in IEC TR 80001-2-2
- **ISO/IEC 80001-xx** including IEC/TR 80001-2-1, IEC/TR 80001-2-3, IEC/TR 80001-2-4, IEC/TR 80001-2-5, ISO/TR 80001-2-6, ISO/TR 80001-2-7 or other
- **EN ISO 62366** / ISO 60601-4 Usability Engineering
- **IEC 62443-4-2** Security for industrial automation and control systems. Part 4-2: Technical security requirements for IACS components.
- **IEC 62443-4-1** Security for industrial automation and control systems. Part 4-1: Secure product development lifecycle requirements.
- **IEC/TR 60601-4-5** Medical Electrical Equipment – Part 4-5. Safety related technical security specifications for medical devices.

Conclusioni

- ✓Le vulnerabilità da cybersecurity derivano dalla presenza di software all'interno di un dispositivo medico.
- ✓Per gestire la natura dinamica del rischio da cybesecurity, il Fabbricante deve applicare la gestione del rischio per tutto il **ciclo di vita** del prodotto.
- ✓Il rischio di cybersecurity deve essere valutato e mitigato nella progettazione, produzione, testing (*fase pre-market*) e durante il monitoraggio post-market.
- ✓La gestione del rischio da cybersecurity deve coinvolgere tutti gli stakeholders che intervengono nelle varie fasi di vita di un dispositivo medico (tra cui le Autorità Competenti).

Grazie per l’attenzione