UNIVERSITÀ
DEGLI STUDI
DI PADOVA

DIPARTIMENTO
DI INGEGNERIA
DELL'INFORMAZIONE

DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE

CORSO DI LAUREA IN INGEGNERIA BIOMEDICA

"Messa in rete dei dispositivi medici: normative, problematiche di interoperabilità e sicurezza"

Relatore: Prof. Giovanni Sparacino

Laureando: Davide Marin

Correlatori: Ing. Massimo Gola, Prof. Simone del Favero

ANNO ACCADEMICO 2022 – 2023

Data di laurea 19-07-2023

INDICE

Sommario

Sommario

Negli ultimi anni si è assistito ad un aumento esponenziale dell'uso dei dispositivi medici connessi alla rete. La messa in rete di tali dispositivi ne comporta l'interconnessione attraverso una rete di comunicazione, come ad esempio una rete LAN o Internet; il fine è quello di consentire la raccolta e lo scambio di dati e informazioni tra i dispositivi, gli operatori sanitari e i pazienti. Questa tendenza è sempre più diffusa nel settore sanitario, in quanto permette di migliorare la qualità e l'efficienza delle cure, nonché di ridurre i costi associati alla gestione dei dati. Tuttavia, la messa in rete dei dispositivi medici presenta anche alcune difficoltà non trascurabili, tra cui la sicurezza e la privacy dei dati, la standardizzazione e l'interoperabilità dei dispositivi e delle infrastrutture di rete. Considerando inoltre che in Italia gli attacchi informatici sono diventati sempre più frequenti e sofisticati [1], diventa chiaro come la messa in rete in sicurezza dei dispositivi medici non può e non deve essere un fattore da trascurare. Il grafico in fig. 1 che segue per esempio mostra il numero di attacchi gravi rilevati in Italia anno per anno tra il 2014 e il 2018 che, come si può ben notare, è aumentato esponenzialmente.

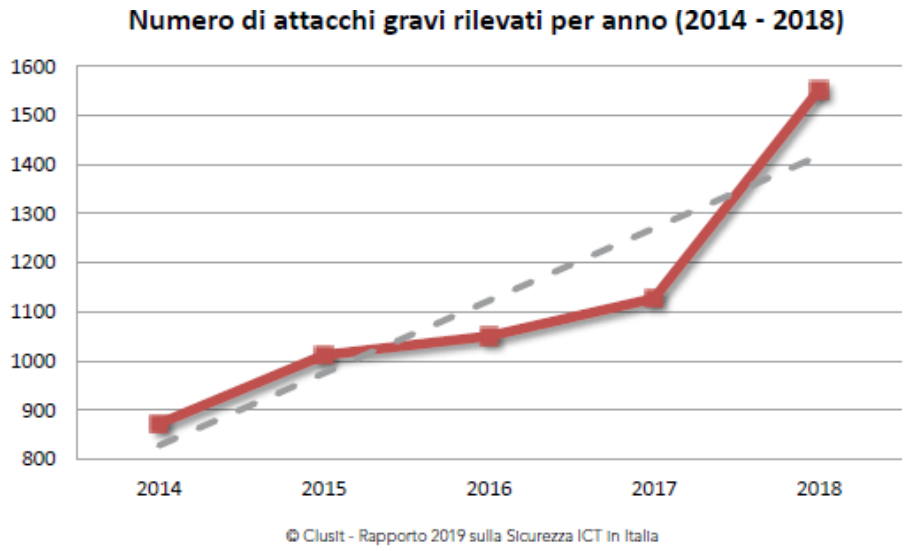

Fig. 1: Numero di attacchi gravi rilevati in Italia

Gli impatti di eventuali attacchi informatici ad una singola struttura sanitaria o al sistema sanitario regionale possono avere ripercussioni più o meno pesanti sia in termini economici, dovendo per esempio investire dei soldi per riparare i sistemi danneggiati, ma soprattutto in termini di salute al cittadino, in quanto ci potrebbero essere interruzioni ai servizi di assistenza come le procedure diagnostiche. A dimostrazione di ciò nel 2008, uno studio condotto da Daniel Halperin [2] ha dimostrato che un defibrillatore cardioverter impiantabile è potenzialmente

suscettibile ad attacchi maligni che violano la privacy delle informazioni dei pazienti e la telemetria medica. Inoltre, il dispositivo potrebbe subire alterazioni dannose all'integrità delle informazioni, compresi i dati dei pazienti e le impostazioni della terapia per quando e come vengono somministrati gli shock.

Per garantire nel dispositivo la sicurezza e la privacy dei dati dovranno quindi essere adottate misure di sicurezza adeguate sia dal produttore che dall'utilizzatore: il primo metterà la sicurezza in primo piano fin dall'inizio del processo di costruzione del dispositivo (sicurezza by design) e configurerà impostazioni di sicurezza predefinite per garantire una maggiore protezione (sicurezza by default); il secondo presterà attenzione all'autenticazione degli utenti, la gestione degli accessi o il cambio di password dopo un periodo prestabilito.

Inoltre, è importante stabilire standard e protocolli comuni per la comunicazione tra i dispositivi, al fine di garantire l'interoperabilità e la compatibilità tra di essi. Nell'ambito medico, i dispositivi devono spesso comunicare tra di loro per scambiarsi informazioni importanti, come i dati dei pazienti o le istruzioni di terapia. Se i dispositivi utilizzano protocolli di comunicazione diversi, potrebbero esserci errori di trasmissione o di interpretazione delle informazioni, che potrebbero portare ad avere gravi conseguenze per la salute dei pazienti. Inoltre, avere protocolli di comunicazione uguali può semplificare l'integrazione dei dispositivi medici in un sistema più ampio, come una rete di monitoraggio della salute o un sistema di gestione delle informazioni sanitarie. Ciò può migliorare l'efficienza del sistema e ridurre il rischio di errori dovuti alla mancanza di compatibilità tra i dispositivi.

1. Dispositivi medici: aspetti introduttivi e scopo dell'elaborato

1.1 Definizione di dispositivo medico

La definizione di dispositivo medico in Italia compare per la prima volta nel Decreto Legislativo n. 46/1997[3]. In particolare, il Decreto prevede che un dispositivo medico è: "qualsiasi strumento, apparecchio, impianto, sostanza o altro prodotto, utilizzato da solo o in combinazione, compreso il software informatico impiegato per il corretto funzionamento, e destinato dal fabbricante ad essere impiegato nell'uomo a scopo di:

- diagnosi, controllo, terapia, attenuazione o compensazione di una ferita o di un handicap
- di studio, sostituzione o modifica dell'anatomia o di un processo fisiologico;
- di intervento sul concepimento, il quale prodotto non eserciti l'azione principale, nel o sul corpo umano, cui è destinato, con mezzi farmacologici o immunologici né mediante processo metabolico ma la cui funzione possa essere coadiuvata da tali mezzi"

Lo stesso Decreto riporta anche la definizione di dispositivo medico in vitro: "qualsiasi dispositivo composto da un reagente, da un prodotto reattivo, da un insieme, da uno strumento, da un apparecchio o da un sistema utilizzato da solo o in combinazione, destinato dal fabbricante ad essere impiegato in vitro per l'esame di campioni provenienti dal corpo umano al fine di fornire informazioni sugli stati fisiologici o sugli stati sanitari o di malattia o anomalia congenita".

Infine, per completezza, viene data anche la definizione di dispositivo medico attivo: "qualsiasi dispositivo medico che richiede una fonte di energia elettrica o di qualsiasi altra forma di energia, diversa dall'energia fornita direttamente dal corpo umano o dalla gravità, per il suo funzionamento principale". Interessante come anche il software di un dispositivo medico rientra in questa categoria.

Solitamente i dispositivi medici sono progettati per essere utilizzati da professionisti sanitari, ma alcuni possono anche essere utilizzati dai pazienti stessi per il monitoraggio o il trattamento di alcune condizioni come, ad esempio, i sistemi di monitoraggio della glicemia. Essi sono soggetti a rigorosi controlli normativi e devono essere approvati dalle autorità competenti prima di poter essere commercializzati. In particolare, in territorio UE un dispositivo medico per poter essere messo in commercio deve riportare il marchio 'CE'. Il marchio CE è un marchio di conformità obbligatorio per i prodotti venduti nell'Unione Europea (UE) e nello Spazio Economico Europeo (SEE). Il marchio CE indica che il prodotto soddisfa i requisiti di sicurezza, salute e ambiente previsti dalla legislazione dell'UE per quel particolare prodotto. Un

dispositivo medico per ottenere quest'ultimo deve soddisfare i requisiti essenziali di sicurezza e di prestazione definiti dal Regolamento sui Dispositivi Medici (MDR) 2017/745[4].

1.2 Classificazione dei dispositivi medici

La classificazione dei dispositivi medici viene stabilita in base al livello di rischio che presentano per la salute dei pazienti e degli operatori sanitari. In Europa, la classificazione viene definita in base alle regole stabilite dal già citato Regolamento sui dispositivi medici (MDR) e dal Regolamento (UE) 2017/746 sui dispositivi medici in vitro (IVDR) [5]. La classificazione di entrambe le tipologie di dispositivi medici si basa sulla valutazione del rischio intrinseco del dispositivo e sulle possibili conseguenze negative per la salute degli utenti in caso di malfunzionamento del dispositivo.

Per quanto riguarda i dispositivi medici la classificazione prevede tre classi:

- Classe I: dispositivi a basso rischio, come termometri, cerotti, garze, ecc. Questi dispositivi sono soggetti a requisiti minimi di sicurezza e di qualità.
- Classe IIa: dispositivi a medio rischio, come gli apparecchi per la pressione sanguigna, gli occhiali per la vista, ecc. Questi dispositivi devono essere soggetti a controlli di qualità più stringenti rispetto ai dispositivi di Classe I.
- Classe IIb: dispositivi a medio-alto rischio, come i defibrillatori, le protesi, gli apparecchi per la radioterapia, ecc. Questi dispositivi devono essere soggetti a controlli di qualità e di sicurezza ancora più rigorosi rispetto ai dispositivi di Classe IIa.
- Classe III: dispositivi ad alto rischio, come i pacemaker, i dispositivi per la dialisi, gli impianti cocleari, ecc. Questi dispositivi richiedono il maggior livello di controlli di qualità e di sicurezza, in quanto possono presentare un rischio grave per la salute dei pazienti se non utilizzati correttamente.

Per i dispositivi medici in vitro, la classificazione viene stabilita sulla base di quattro classi:

- Classe A: dispositivi medici in vitro a basso rischio, ad esempio i test per la gravidanza.
- Classe B: dispositivi medici in vitro a medio-basso rischio, ad esempio i test per la diagnosi di infezioni batteriche o virali.
- Classe C: dispositivi medici in vitro a medio-alto rischio, ad esempio i test per la diagnosi di malattie autoimmuni o genetiche.
- Classe D: dispositivi medici in vitro ad alto rischio, ad esempio i test per la diagnosi di malattie oncologiche o infettive.

1.3 Scopo dell'elaborato e presentazione

Dopo aver dato una definizione di dispositivi medici e la loro relativa classificazione nel primo capitolo, nel secondo capitolo verranno descritte le principali normative e direttive in campo europeo per quanto riguarda i dispositivi medici. In particolare, si approfondirà:

- il Regolamento (UE) sui dispositivi medici (MDR);
- il Regolamento generale sulla protezione dei dati (GDPR), particolarmente importante quando si ha bisogno di trattare i dati sensibili dei pazienti;
- Direttiva NIS Network and Information Security, che mira a migliorare la sicurezza informatica sul territorio europeo

Nel terzo capitolo verrà illustrato un piano di messa in rete e integrazione fra dispositivi medici. In particolare, verranno dati una serie di accorgimenti da rispettare per una messa in sicurezza dei dispositivi medici nella rete ospedaliera e una serie di standard internazionali di integrazione fra dispositivi medici (ICD9-CM, HL7, DICOM).

Nel quarto capitolo verrà illustrato lo stato dell'arte dei sistemi di rete e come aumentarne la sicurezza.

Infine, nel quinto e ultimo capitolo verrà proposto un caso di studio di messa in rete di un sistema cardiotocografico, svolto durante il tirocinio presso 'Sistemi informativi' dell'AULSS4.

2. Normative inerenti ai dispositivi medici: MDR, GDPR e direttiva NIS

2.1 Regolamento sui dispositivi medici (MDR)

Il Regolamento sui dispositivi medici è un regolamento dell'Unione Europea che disciplina la commercializzazione dei dispositivi medici all'interno dell'UE. Entrato in vigore il 26 maggio 2021, sostituisce la precedente Direttiva sui dispositivi medici (Medical Device Directive) e la Direttiva sui dispositivi medici impiantabili attivi (Active Implantable Medical Device Directive).

Introduce importanti cambiamenti al sistema di regolamentazione dei dispositivi medici in Europa, al fine di garantire la sicurezza e l'efficacia dei dispositivi medici, nonché di rafforzare la trasparenza e la tracciabilità dei prodotti. In particolare, il regolamento introduce nuovi requisiti per la certificazione dei dispositivi medici, la sorveglianza del mercato e la vigilanza post-commercializzazione.

Il Regolamento amplia innanzitutto la definizione di dispositivo medico, sino a includervi anche dispositivi che non hanno uno scopo medico previsto come, ad esempio, lenti a contatto colorate o che precedentemente non erano considerati dispositivi medici come i software dei dispositivi. Viene poi, come già visto, effettuata una nuova classificazione dei dispositivi medici oltre che introdurre la codifica UDI (identificazione univoca dei dispositivi) per consentirne una migliore tracciabilità e facilitare l'eventuale ritiro di dispositivi che presentino un rischio per la sicurezza. La codifica UDI richiede che ogni dispositivo medico sia contrassegnato con un codice univoco, che contiene informazioni come il produttore, il modello e il numero di lotto. Questo sistema aiuta a migliorare la tracciabilità dei dispositivi medici e a facilitare la loro identificazione in caso di richiami di sicurezza o di altre problematiche.

Viene prevista una vigilanza più rigorosa da parte degli Organismi notificati, ovvero organizzazioni private o pubbliche, che sono state autorizzate e notificate dalla Commissione Europea per svolgere determinate attività di valutazione della conformità dei prodotti. Gli organismi notificati svolgono diverse funzioni, tra cui la valutazione della conformità dei prodotti, la certificazione, il collaudo e l'ispezione.

Viene creata la banca dati europea sui dispositivi medici (Eudamed) per fornire un accesso più efficiente alle informazioni sui dispositivi medici approvati. Tale piattaforma sarà composta da sei sezioni per la registrazione degli operatori economici, dei dispositivi medici, degli Organismi notificati, indagini cliniche e studi delle presentazioni, vigilanza e sorveglianza post-commercializzazione e sorveglianza del mercato.

Vengono inoltre definiti gli attori del sistema dei dispositivi medici. Il Medical Device Regulation (MDR) definisce innanzitutto il 'fabbricante' come: "la persona fisica o giuridica che fabbrica o rimette a nuovo un dispositivo oppure lo fa progettare, fabbricare o rimettere a nuovo, e lo commercializza apponendovi il suo nome o marchio commerciale". Quest'ultimo ha la responsabilità giuridica del prodotto ed è tenuto a costituire il fascicolo tecnico del fabbricante contenente tutte le informazioni richieste. Il fabbricante deve inoltre garantire che i dispositivi da lui immessi in commercio siano conformi ai requisiti generali di prestazione e sicurezza definiti dal Regolamento, nonché effettuare la valutazione clinica prevista al fine di dimostrare il rispetto dei requisiti di sicurezza e prestazione del dispositivo medico, la sua idoneità al raggiungimento della destinazione d'uso, la valutazione degli eventuali effetti collaterali. Conclusa la fase di realizzazione e valutazione della conformità del dispositivo, il fabbricante dovrà redigere la documentazione tecnica, apporre il marchio CE, assegnare un codice UDI al prodotto, iscriverlo nella banca dati Eudamed e realizzare l'etichettatura. Per quanto riguarda gli obblighi post-commercializzazione il fabbricante, al fine di garantire la massima tracciabilità del dispositivo, è tenuto a realizzare un piano di sorveglianza post-commercializzazione e ad adottare procedure interne per la segnalazione all'autorità competente tramite la banca dati Eudamed di qualsiasi incidente grave e/o azione correttiva di sicurezza. Quando il fabbricante di un dispositivo medico ha sede in un territorio extra UE l'immissione in commercio avviene ad opera 'dell'importatore', ovvero: "qualsiasi persona fisica o giuridica stabilita nell'Unione che immette sul mercato dell'Unione un dispositivo originario di un paese terzo", e del "distributore", ovvero: 'qualsiasi persona fisica o giuridica nella catena di fornitura, diversa dal fabbricante o dall'importatore, che mette a disposizione sul mercato un dispositivo, fino al momento della messa in servizio". Entrambe le figure non erano disciplinate dalla precedente normativa. Su importatore e distributore grava l'obbligo di controllare la conformità del dispositivo al MDR ed un generale obbligo di cooperazione con le autorità competenti per qualsiasi azione volta ad eliminare o attenuare i rischi eventualmente presentati da dispositivi commercializzati. Il Regolamento rafforza poi, rispetto alla previgente disciplina, la figura del 'mandatario' ossia: "il soggetto nominato da un fabbricante extra-UE e da questi autorizzato ad agire sul territorio comunitario per suo conto mediante accordo scritto". Il MDR prevede che il mandatario è tenuto al controllo formale della documentazione comprovante la conformità del dispositivo medico ed è obbligato alla registrazione in Eudamed oltre che al controllo dell'avvenuta registrazione del fabbricante e del dispositivo medico. Esso inoltre è responsabile in solido con il fabbricante per eventuali dispositivi medici difettosi immessi in commercio.

2.2 Regolamento generale sulla protezione dei dati (GDPR)

Il Regolamento Generale sulla Protezione dei Dati (GDPR) [6] è un regolamento dell'Unione Europea che disciplina la protezione dei dati personali dei cittadini dell'Unione Europea. Il regolamento è entrato in vigore il 25 maggio 2018, sostituendo la Direttiva 95/46/CE sulla protezione dei dati personali. Il GDPR definisce i requisiti dettagliati per le aziende e le organizzazioni in materia di raccolta, archiviazione e gestione dei dati personali. Valgono sia per le organizzazioni europee che trattano i dati personali dei cittadini nell'UE sia per le organizzazioni esterne all'UE che si rivolgono a persone che vivono nell'UE. L'obiettivo è dunque quello di rafforzare la protezione dei dati per tutte le persone le cui informazioni personali rientrano nel suo campo di applicazione, dando loro il pieno controllo dei propri dati.
Il GDPR definisce i dati personali come: "qualsiasi informazione relativa a una persona fisica identificata o identificabile". Ciò significa che qualsiasi informazione che può essere utilizzata per identificare una persona fisica, direttamente o indirettamente, costituisce un dato personale. I dati personali possono includere nome, indirizzo, indirizzo email, numero di telefono, foto, indirizzo IP, informazioni sulla posizione, informazioni mediche, informazioni finanziarie e altro ancora. Inoltre, il GDPR riconosce anche che i dati personali possono essere sensibili, ovvero: "qualsiasi informazione relativa a una persona fisica che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, lo stato di salute o la vita sessuale o l'orientamento sessuale della persona". Per questa tipologia di dati il regolamento prevede protezioni speciali.
Vengono inoltre date altre importanti definizioni:

- Titolare del trattamento: "la persona fisica o giuridica, l'autorità pubblica, l'agenzia o qualsiasi altro organismo che, da solo o insieme ad altri, determina le finalità e i mezzi del trattamento dei dati personali";
- Responsabile del trattamento: "la persona fisica o giuridica, l'autorità pubblica, l'agenzia o qualsiasi altro organismo che tratta i dati personali per conto del titolare del trattamento";
- Interessato: "la persona fisica cui si riferiscono i dati personali".

Il GDPR si applica quando:

- la base operativa dell'organizzazione si trova nell'Unione Europea (ciò vale indipendentemente dal fatto che il trattamento abbia luogo nel territorio UE o meno);
- l'organizzazione, seppure non avente sede nell'Unione Europea, offre beni o servizi (anche gratuitamente) a cittadini europei. Può trattarsi di enti pubblici, società private o pubbliche, persone fisiche od organizzazioni senza scopo di lucro;

- l’organizzazione, seppure non avente sede nell’Unione Europea, monitora il comportamento delle persone che vi risiedono, a patto che tale comportamento abbia luogo all’interno del territorio UE.

Un ambito di applicazione così ampio copre in pratica quasi tutte le attività, e pertanto si può concludere che il GDPR si applica indipendentemente dal fatto che la tua organizzazione si trovi o meno nell’Unione Europea.

Il GDPR prevede che i dati possono essere trattati solo se sussiste almeno una base giuridica del trattamento come, per esempio, quando c’è il consenso inequivocabile da parte dell’utente per una o più specifiche finalità. Poiché il consenso ai sensi del GDPR è una questione di primaria importanza, è obbligatorio registrare in modo puntuale i consensi ottenuti affinché l’organizzazione sia in grado di dimostrare che l’utente abbia effettivamente prestato il consenso.

Il GDPR definisce una serie di diritti dell’utente:

- Il diritto ad essere informati: le organizzazioni devono fornire agli utenti informazioni sulle attività di trattamento dei dati che svolgono;
- Il diritto di accesso: gli utenti hanno il diritto di accedere ai propri dati personali e alle informazioni relative alle modalità di trattamento degli stessi. Su richiesta dell’utente, i titolari del trattamento devono fornire una panoramica delle categorie di dati trattati, una copia degli effettivi dati raccolti ed una descrizione delle modalità del trattamento. È necessario chiarire inoltre le finalità del trattamento, il modo in cui i dati sono stati acquisiti e i soggetti con cui i dati sono stati eventualmente condivisi;
- Il diritto di rettifica: gli utenti hanno il diritto di richiedere la rettifica dei loro dati personali se sono imprecisi o incompleti. Questo diritto implica anche che la rettifica debba essere comunicata a tutti i soggetti terzi coinvolti nel trattamento dei dati in questione, a meno che ciò non sia impossibile o particolarmente difficile;
- Il diritto di opporsi: gli utenti hanno il diritto di opporsi a determinate attività di trattamento dei loro dati personali effettuate dal titolare del trattamento;
- Il diritto alla cancellazione: quando i dati non sono più utili per le finalità per le quali sono stati raccolti, in caso di revoca del consenso da parte dell’utente o quando i dati personali sono stati trattati in modo illecito, l’utente ha il diritto di chiederne la cancellazione nonché la cessazione di ogni altra forma di diffusione.

Inoltre, vengono introdotti due importanti concetti ovvero la "privacy by design" e la "privacy by default". Privacy by design significa che la privacy viene presa in considerazione durante l'intero processo di sviluppo di un prodotto o servizio, dalla fase di progettazione alla fine del

suo ciclo di vita. Privacy by default significa che la privacy viene automaticamente integrata nel prodotto o servizio, in modo che gli utenti non debbano compiere ulteriori passi per proteggere le loro informazioni personali. Nella pratica, la privacy by design significa che le organizzazioni dovrebbero considerare i rischi per la privacy e implementare le adeguate garanzie quando progettano nuovi prodotti o servizi, anziché affrontare le preoccupazioni sulla privacy come un'aggiunta successiva. Ciò può includere l'integrazione di funzioni di privacy come la crittografia e i controlli di accesso, la minimizzazione della quantità di dati personali raccolti e l'implementazione di politiche per garantire che i dati personali vengano utilizzati solo per la loro finalità prevista. La privacy by default significa che le organizzazioni dovrebbero assicurarsi che le impostazioni sulla privacy siano impostate per impostazione predefinita sulla maggior parte delle opzioni di privacy, invece di richiedere agli utenti di regolare manualmente le impostazioni per proteggere i loro dati personali. Ciò può includere impostazioni come la limitazione della conservazione dei dati personali, la minimizzazione della quantità di dati personali raccolti e la fornitura agli utenti di politiche sulla privacy chiare e facili da comprendere.

2.2.1 Il Data Protection Impact Assessment (DPIA)

Il Data Protection Impact Assessment (DPIA) è un processo utilizzato per aiutare le organizzazioni a rispettare efficacemente il GDPR e a garantire che i principi di responsabilità, privacy by design e privacy by default siano effettivamente messi in pratica dall'organizzazione. Il processo di DPIA deve essere documentato per iscritto.

Sebbene la pubblicazione del DPIA non sia un obbligo formale imposto dal GDPR, è auspicabile che i titolari del trattamento prendano in considerazione l'opportunità di pubblicare in tutto o in parte le loro DPIA come segno di trasparenza e responsabilità, soprattutto nei casi in cui siano coinvolti soggetti pubblici (ad esempio, quando la DPIA è effettuata da un ente pubblico).

Attuare degli efficaci processi di DPIA è utile per soddisfare il requisito della "privacy by design" in quanto consente alle organizzazioni di individuare e risolvere i problemi in una fase precoce, riducendo così sia i rischi per la sicurezza dei dati degli utenti, sia il rischio di sanzioni e di danni reputazionali che potrebbero altrimenti verificarsi per l'organizzazione.

In generale, la DPIA è obbligatoria solo nei casi in cui l'attività di trattamento dei dati è suscettibile di comportare un rischio elevato per gli utenti. Tuttavia, se non si è sicuri che la propria attività di trattamento rientri o meno in quello che viene considerato un "rischio elevato", si raccomanda di effettuare comunque una DPIA, in quanto si tratta di uno strumento utile a garantire il rispetto della legge.

Le attività di trattamento dei dati considerate ad "alto rischio" includono:

- il trattamento di dati sensibili;
- il monitoraggio sistematico di un'area accessibile al pubblico (ad esempio, tramite video sorveglianza);
- le situazioni in cui vengono effettuate valutazioni automatizzate e approfondite dei dati personali al fine di influenzare in modo significativo decisioni rilevanti per la vita dell'utente.

Le valutazioni d'impatto possono essere richieste anche in altre circostanze (sulla base di una valutazione caso per caso), tra cui il trattamento dei dati relativi a persone vulnerabili (come bambini o anziani), il trasferimento di dati al di fuori del territorio UE e il trattamento di dati utilizzati per la profilazione.

La relazione prodotta a seguito di un processo di DPIA dovrebbe includere:

- una descrizione completa dei dati trattati;
- lo scopo dell'attività di trattamento (e, se del caso, le informazioni sugli interessi legittimi del responsabile del trattamento);
- una valutazione dell'ambito e della necessità dell'attività di trattamento in relazione alla finalità perseguita;
- una valutazione del rischio per gli utenti;
- le misure in atto per far fronte a tale rischio.

2.2.2 Coordinamento tra MDR e GDPR

È evidente che i moderni dispositivi medici, spesso connessi alla rete o costituiti da software o app, sono in grado di trattare importanti quantità di dati personali relativi alla salute e la corretta gestione di tali dati diventa allora un necessario requisito di sicurezza del dispositivo stesso. Ogni attore del sistema dei dispositivi medici, in base al tipo di dati raccolti, dovrà determinare proprie policy per raggiungere la conformità al GDPR che tengano conto dei diritti degli interessati, della necessità di utilizzare i dati solo per gli scopi per i quali siano stati raccolti, dell'implementazione di adeguate misure tecniche organizzative per la protezione dei dati e per assicurare idonee procedure per la rilevazione delle violazioni.

Il MDR, nell'elencare i requisiti di sicurezza e progettazione che devono essere rispettati da dispositivi che contengono un software o che siano essi stessi un software, prevede che siano sviluppati e fabbricati tenendo conto della sicurezza delle informazioni, che i fabbricanti indichino le caratteristiche delle reti informatiche e le misure di sicurezza informatica,

compresa la protezione contro l'accesso non autorizzato necessari per far funzionare il dispositivo.

2.3 Direttiva sulla sicurezza delle reti e dei sistemi informativi (Direttiva NIS)

La Direttiva sulla sicurezza delle reti e dei sistemi informativi, conosciuta come Direttiva NIS (Network and Information Security), è una direttiva dell'Unione Europea entrata in vigore il 10 maggio 2018. La Direttiva si applica agli Operatori dei servizi essenziali (OES), ovvero imprese che forniscono servizi essenziali per la società e l'economia come il sistema sanitario e le infrastrutture digitali, e ai Fornitori di servizi digitali (FSD), ovvero imprese che offrono servizi digitali come i motori di ricerca. La Direttiva NIS ha lo scopo di rafforzare la sicurezza informatica in tutti quei settori a cui quest'ultima è rivolta.

In particolare, la direttiva NIS prevede:

- Misure di sicurezza informatica: i fornitori di servizi essenziali e le infrastrutture critiche devono adottare misure di sicurezza adeguate a prevenire e gestire gli incidenti informatici, come ad esempio l'utilizzo di sistemi di autenticazione robusti, l'implementazione di politiche di gestione dei rischi informatici e la designazione di responsabili della sicurezza informatica;
- Notifica degli incidenti informatici: i fornitori di servizi essenziali e le infrastrutture critiche devono notificare le autorità competenti degli incidenti informatici rilevanti entro un determinato periodo di tempo e devono collaborare con queste autorità per risolvere il problema;
- Cooperazione tra Stati membri: gli Stati membri dell'UE devono cooperare tra di loro per garantire un elevato livello di sicurezza informatica per i servizi essenziali e le infrastrutture critiche a livello transfrontaliero.
- Sanzioni: gli Stati membri devono prevedere sanzioni appropriate per i fornitori di servizi essenziali che non rispettano gli obblighi previsti dalla direttiva.

L'approccio migliore per i FSD e gli OES per essere conformi è implementare un programma di cyber resilienza che includa i seguenti punti:

- Difese solide per la cyber sicurezza;
- Misure preventive adeguate contro il cyber rischio;
- Strumenti e sistemi adeguati per gestire e segnalare incidenti e violazioni dei dati.

Per quanto riguarda l'Italia e in particolare il sistema sanitario, il ministero della salute [8] in quanto autorità competente NIS per il settore salute ha:

- individuato gli OSE

- ha emesso le Linee guida OSE

Le Linee guida per gli OSE costituiscono uno strumento operativo di supporto al processo di gestione e trattamento del rischio cyber, per affrontare in modo organico e qualificato la gestione della sicurezza delle reti e dei sistemi informativi. A tale scopo sono basate sul Framework Nazionale per la Cyber Security e la Data Protection [9], nel cui ambito è possibile inquadrare le misure di sicurezza, gli standard e le norme di settore, senza imporre agli operatori l'impiego di una specifica dotazione strumentale, bensì suggerendo un approccio razionale e dinamico strettamente legato all'analisi del rischio.

Il 14 dicembre 2022 la direttiva NIS è stata sostituita dalla Commissione europea con la cosiddetta NIS2 (Direttiva n. 2555/2022[10]) al fine di rispondere alle crescenti minacce poste dalla digitalizzazione e all'ondata di attacchi informatici. La direttiva NIS2 amplia i settori e le tipologie di entità critiche che rientrano nel campo di applicazione, comprendendo, per esempio, gli enti della pubblica amministrazione. Sono stati rafforzati i requisiti di gestione del rischio di sicurezza informatica che le aziende sono tenute a rispettare e sono stati snelliti gli obblighi di segnalazione degli incidenti con disposizioni più precise in materia di segnalazione, contenuto e tempistica.

Tra i capisaldi della direttiva NIS2 ci sono:

- rideterminazione e ampliamento dell'ambito di applicazione delle norme in materia di sicurezza dei dati;
- potenziamento degli organi e delle attività di supervisione a livello comunitario, con l'obiettivo di migliorare la collaborazione per contrastare la minaccia informatica globale, grazie alla condivisione delle esperienze tra gli stati membri;
- razionalizzazione dei requisiti minimi di sicurezza e delle procedure di notifica obbligatoria degli incidenti informatici;
- estensione dei concetti di gestione del rischio e di valutazione delle vulnerabilità a tutta la supply chain, coinvolgendo tutti o un maggior numero di stakeholder coinvolti.

2.3.1 Framework Nazionale per la Cyber Security e la Data Protection

Il Framework Nazionale per la Cybersecurity e la Data Protection rappresenta uno strumento di misura della postura di sicurezza di un'organizzazione in termini di maturità e completamento di attività volte a ridurre il rischio cibernetico. Pubblicato in Italia nel 2015 e aggiornato nel 2019 alla versione 2.0 al fine di cogliere gli aspetti legati alla Data Protection espressi nel GDPR, il Framework consente di approfondire diverse dimensioni inerenti alla cybersecurity. Ideato per essere fruibile da organizzazioni pubbliche e private di diverse dimensioni, il Framework è caratterizzato da una serie di elementi cardine, che riprendono e

integrano quanto proposto dal NIST [11] (National Institute of Standards and Technology) con il suo Cybersecurity Framework:

- Core: elenco strutturato di requisiti necessari per raggiungere diversi obiettivi di sicurezza. Sono organizzati in function (identify, protect, detect, respond, recover), category e subcategory;
- Controlli: insieme di azioni in cui si possono declinare i requisiti espressi dalla subcategory. Sono da definire in base alle caratteristiche ed alle necessita di ciascuna organizzazione;
- Informative references: riferimenti che legano ogni singola subcategory a pratiche di sicurezza note previste da regolamentazioni generali vigenti e da standard di settore;
- Livelli di priorità: livelli che indicano la priorità di implementazione delle prescrizioni indicate in ogni subcategory;
- Livelli di maturità: livelli di maturità implementativa di subcategory e controlli;
- Contestualizzazione: processo di selezione delle subcategory di interesse per l'organizzazione e di valutazione dei livelli di priorità e di maturità per le subcategory selezionate;
- Prototipo di contestualizzazione: template di supporto per attuare con contestualizzazione, basati sulle indicazioni fornite dalle informative reference.

Il Framework presenta tre fasi:

1. Contestualizzazione: questa prima fase ha l'obiettivo di contestualizzare il Framework alla realtà di interesse. In particolare, si selezionano e valutano, in termini di maturità e priorità, le subcategory di interesse rispetto alla realtà di riferimento attraverso la combinazione di prototipi di contestualizzazione esistenti. Il prodotto di questa fase sarà un Profilo Target, ovvero il riferimento desiderato al quale tendere. La sua corretta definizione è quindi funzionale allo svolgimento delle successive due fasi;
2. Misura: in questa seconda fase si procede a individuare l'attuale postura di sicurezza cyber dell'organizzazione rispetto a quanto definito nel Profilo Target. Tale processo avviene attraverso interviste a soggetti competenti per le specifiche esigenze di analisi. Il risultato delle interviste viene espresso in termini di copertura e maturità per ogni controllo individuato;
3. Valutazione: nella terza fase si ha una valutazione della distanza dall'obbiettivo desiderato. Il risultato da un punteggio di completamento delle azioni individuate e in un ulteriore punteggio che rappresenta il grado di maturità con cui le suddette azioni sono realizzate.

3. Piano di messa in rete e integrazione fra dispositivi medici

3.1 Piano di messa in rete dei dispositivi medici

Un piano di messa in rete dei dispositivi medici è un piano che descrive come i dispositivi medici saranno collegati in rete all'interno di un'infrastruttura sanitaria.

In particolare, il piano dovrebbe specificare come i dispositivi saranno collegati tra loro e alla rete di comunicazione dell'ospedale o della struttura sanitaria, così come le procedure e le politiche di sicurezza che saranno implementate per garantire la protezione dei dati dei pazienti e la sicurezza dell'infrastruttura di rete. Il piano dovrebbe anche descrivere come i dati saranno raccolti, archiviati e utilizzati per supportare la cura dei pazienti e la gestione delle informazioni sanitarie. Inoltre, dovrebbe includere anche un piano per la manutenzione e la gestione dei dispositivi collegati in rete, nonché un piano di formazione per il personale medico e tecnico che utilizzerà i dispositivi.

Il collegamento dei dispositivi medici alla rete ospedaliera può migliorare la qualità delle cure, aumentare l'efficienza, ridurre gli errori e garantire la sicurezza dei pazienti. In particolare, i vantaggi di dispositivi medici collegati alla rete ospedaliere sono:

- Monitoraggio e raccolta di dati: i dispositivi medici collegati alla rete ospedaliera possono inviare dati in tempo reale ai sistemi informatici dell'ospedale. Ciò consente ai medici e al personale sanitario di monitorare i pazienti e raccogliere dati sulle loro condizioni in modo più accurato ed efficiente.
- Migliore qualità delle cure: la raccolta di dati in tempo reale consente ai medici di prendere decisioni cliniche più informate e di adottare interventi più precoci e appropriati, migliorando la qualità delle cure.
- Miglioramento dell'efficienza: l'uso di dispositivi medici collegati alla rete ospedaliera può ridurre i tempi di attesa e migliorare l'efficienza delle procedure mediche. Inoltre, ciò può contribuire a ridurre gli errori umani associati alla raccolta manuale dei dati.
- Risparmio di tempo: l'invio automatico dei dati dei pazienti ai sistemi informatici dell'ospedale consente di risparmiare tempo e risorse.
- Maggiore sicurezza: la connessione dei dispositivi medici alla rete ospedaliera può consentire di monitorare costantemente i dispositivi stessi, individuare eventuali problemi o malfunzionamenti e garantire la sicurezza dei pazienti.

Un importante standard in questo ambito è l'IEC 80001 [12], intitolato "Sistemi informativi sanitari - Applicazione delle pratiche di gestione del rischio per la sicurezza dell'IT". Questo standard fornisce linee guida per l'identificazione, l'analisi e la gestione dei rischi associati

all'utilizzo di sistemi informativi sanitari, compresi i dispositivi medici connessi in rete. Un piano per la messa in rete dei dispositivi medici dovrebbe prevedere diverse fasi e considerare diversi aspetti, tra cui:

- Valutazione dei rischi: valutare i rischi associati alla messa in rete dei dispositivi medici, come il rischio di hackeraggio, la perdita di dati o la violazione della privacy dei pazienti. Questa valutazione può aiutare a identificare le misure di sicurezza necessarie per mitigare i rischi;
- Utilizzare una rete separata: creare una rete separata e dedicata solo ai dispositivi medici. Questo separa il traffico dei dispositivi medici dal traffico dei dispositivi non medici e fornisce un livello aggiuntivo di sicurezza;
- Utilizzare dispositivi sicuri: scegliere dispositivi medici che rispettino gli standard di sicurezza richiesti. Inoltre, verificare che i dispositivi siano dotati di un sistema di sicurezza integrato e che vengano regolarmente aggiornati con le ultime patch di sicurezza;
- Controllo degli accessi: limitare l'accesso alla rete ai soli dispositivi medici autorizzati e alle persone autorizzate può aiutare a prevenire accessi non autorizzati;
- Monitorare il traffico di rete: monitorare costantemente il traffico di rete dei dispositivi medici per rilevare eventuali attività sospette. Ciò può aiutare a identificare rapidamente eventuali violazioni della sicurezza e adottare le necessarie misure correttive;
- Verifica dell'identità: l'autenticazione dell'utente e la verifica dell'identità sono essenziali per garantire che solo le persone autorizzate possano accedere ai dati dei pazienti e controllare i dispositivi medici;
- Proteggere le password: utilizzare password complesse e uniche per i dispositivi medici e cambiarle regolarmente. Inoltre, utilizzare la crittografia per proteggere le password durante la trasmissione;
- Formare il personale: fornire formazione regolare ai professionisti sanitari e ai tecnici che utilizzano i dispositivi medici sulla sicurezza informatica e sui protocolli per prevenire le violazioni della sicurezza;
- Creare una politica di sicurezza: creare una politica di sicurezza informatica dettagliata per la gestione dei dispositivi medici. Questo dovrebbe includere procedure per la sicurezza dei dati, l'accesso ai dispositivi e la gestione degli aggiornamenti di sicurezza;
- Monitoraggio continuo: monitorare continuamente la rete e i dispositivi medici connessi per individuare eventuali problemi o guasti e intervenire tempestivamente per ripristinare il corretto funzionamento del sistema;

- Gestione dei dati: definire una politica di gestione dei dati dei pazienti che includa la conservazione, la condivisione il backup e la cancellazione dei dati per garantire la privacy e la protezione dei dati sensibili dei pazienti.

3.2 Integrazione fra dispositivi medici e problematiche di interoperabilità

L'integrazione fra dispositivi medici si riferisce alla capacità dei diversi dispositivi medici di comunicare tra loro e scambiarsi informazioni. Questo permette di migliorare l'efficacia e la sicurezza dei trattamenti medici, ridurre gli errori di diagnosi e terapia e ottimizzare la gestione dei dati medici. L'uso di standard di comunicazione condivisi tra i dispositivi medici, come ad esempio l'HL7 (Health Level Seven) o il DICOM (Digital Imaging and Communications in Medicine), facilita l'integrazione e lo scambio di informazioni tra i vari sistemi. L'integrazione dei dispositivi medici è particolarmente importante in ambito ospedaliero, dove si utilizzano numerosi dispositivi medici diversi che, potenzialmente, potrebbero avere standard di comunicazione diversi fra loro. L'integrazione di questi dispositivi permette di avere una visione più completa e dettagliata dello stato del paziente, migliorando la capacità di diagnosi e la qualità dell'assistenza medica. Inoltre, l'integrazione dei dispositivi medici può essere utile anche fuori dall'ospedale, ad esempio per monitorare i pazienti a distanza o per gestire la terapia domiciliare. Ciò consente di ridurre i costi sanitari e di migliorare la qualità della vita dei pazienti.

Per garantire l'interoperabilità bisogna assicurare una:

- standardizzazione semantica: questo tipo di standardizzazione si concentra sulla definizione di un insieme comune di significati per i dati sanitari. Ciò significa che tutte le informazioni sono interpretate nello stesso modo, indipendentemente dal contesto o dal sistema informatico in cui vengono utilizzate. L'obiettivo della standardizzazione semantica è di garantire che i dati sanitari siano compresi in modo uniforme da tutti i professionisti del settore;
- standardizzazione terminologica: questo tipo di standardizzazione si concentra sulla definizione di un insieme comune di termini e abbreviazioni per i dati sanitari. Ciò significa che tutti i professionisti del settore utilizzano gli stessi termini per descrivere le stesse condizioni o procedure. L'obiettivo della standardizzazione terminologica è di evitare la confusione causata dall'uso di termini diversi per riferirsi alla stessa cosa. Un esempio è lo standard ICD9-CM;
- standardizzazione sintattica: questo tipo di standardizzazione si concentra sulla definizione di un insieme comune di regole per la struttura dei dati sanitari. Ciò significa che tutti i dati sono organizzati in modo uniforme e coerente, il che facilita

l'interoperabilità tra diversi sistemi informatici. L'obiettivo della standardizzazione sintattica è di garantire che i dati sanitari possano essere scambiati in modo affidabile tra diversi sistemi informatici, senza rischio di errori o fraintendimenti. Un esempio è lo standard HL7.

3.2.1 ICD9-CM

La Classificazione internazionale delle malattie (ICD) è un sistema di classificazione che organizza le malattie ed i traumatismi in gruppi sulla base di criteri definiti. La Classificazione internazionale, sottoposta a periodiche revisioni, fu adottata anche per rilevare le cause di morbosità oltre che di mortalità. Nel 1975, a Ginevra, nel corso della 29ª Assemblea della Organizzazione Mondiale della Sanità fu approvata la nona revisione della Classificazione (ICD-9). Dal 1979, negli Stati Uniti, un Comitato, formato dalle associazioni professionali ed accademiche dei medici, ha sviluppato e provvede ad aggiornare annualmente una versione modificata ed ampliata, con l'introduzione degli interventi e delle procedure diagnostiche e terapeutiche, del sistema di classificazione, la ICD-9-CM [13] International Classification of Diseases, 9th revision, Clinical Modification. Da allora, nell'ottobre di ciascun anno viene pubblicato un aggiornamento dell'ICD-9-CM. Il termine clinical è utilizzato per sottolineare le modifiche introdotte: rispetto alla ICD-9, fortemente caratterizzata dall'orientamento a scopo di classificazione delle cause di mortalità, la ICD-9-CM è soprattutto orientata a classificare le informazioni sulla morbosità. Infatti, le principali modifiche sono finalizzate a consentire sia una classificazione più precisa ed analitica delle formulazioni diagnostiche sia l'introduzione della classificazione delle procedure diagnostiche e terapeutiche.

La classificazione ICD-9-CM descrive in codici numerici o alfa-numerici i termini medici in cui sono espressi le diagnosi di malattia o di traumatismo, gli altri problemi di salute, le cause di traumatismo e le procedure diagnostiche e terapeutiche. Le caratteristiche fondamentali della ICD-9-CM sono le seguenti:

- l'esaustività: tutte le entità trovano una loro collocazione, più o meno specifica, entro i raggruppamenti finali della classificazione;
- la mutua esclusività: ciascuna entità è classificabile soltanto in uno dei raggruppamenti finali della classificazione;
- il numero limitato di raggruppamenti: circa 16.000 codici consentono la classificazione delle diagnosi, dei problemi di salute e delle principali procedure diagnostiche e terapeutiche;

La struttura della classificazione è determinata da due assi principali, l'eziologia e la sede anatomica. I capitoli in cui si articola la classificazione riflettono i due assi principali: il criterio

eziologico determina i cosiddetti capitoli speciali (malattie infettive, malattie costituzionali e generali, malattie dello sviluppo, traumi); il criterio anatomico determina i capitoli cosiddetti locali, ovvero riferiti ad una specifica sede anatomica. In generale il criterio eziologico prevale su quello anatomico, per cui le condizioni morbose sono in via prioritaria classificate in uno dei capitoli speciali. In ICD-9-CM le informazioni, relative a 13000 diagnosi e oltre 3000 interventi e procedure, sono organizzate in modo gerarchico, in cui i concetti vanno dal generale allo specifico. In particolare, per le 13000 diagnosi, la classificazione parte da 17 capitoli. Ogni capitolo è a sua volta suddiviso in diversi blocchi. Ad ogni filiazione, nel codice c'è l'aggiunta a destra di un carattere numerico e, più un concetto è specifico, più è complesso il suo codice. I codici ICD-9-CM per le diagnosi sono costituiti da 3 a 5 caratteri alfanumerici. Quando sono necessari più di tre caratteri, un punto decimale è interposto tra il terzo e il quarto carattere. In particolare, abbiamo:

- Blocco: insieme di condizioni tra loro strettamente correlate;
- Categoria: codici a tre caratteri, alcuni dei quali già molto specifici e non ulteriormente suddivisibili, mentre altri sono ulteriormente suddivisi, con l'aggiunta di un quarto carattere dopo il punto decimale;
- Sottocategoria: codici a quattro caratteri, il quarto carattere fornisce ulteriore specificità o informazione relativamente ad eziologia, localizzazione o manifestazione clinica;
- Sotto-classificazioni: codici a cinque caratteri.

3.2.2 Standard HL7 e FHIR

Lo standard HL7 (Health Level Seven) [14] è uno standard approvato per la generazione di messaggi standardizzati, il suo nome deriva dal particolare livello 7 dello standard ISO/OSI (International Standards Organization/ Open System Interconnection) per le telecomunicazioni. Nasce alla fine degli anni '80 con lo scopo di uniformare e semplificare lo scambio elettronico di informazioni cliniche ed amministrative tra i diversi sistemi presenti in un'azienda sanitaria. Lo standard HL7 viene sviluppato ed aggiornato da un comitato di utenti e produttori con l'obiettivo comune di semplificare le interfacce tra applicazioni di produttori diversi, spesso antagonisti, ed uniformare il formato e il protocollo utilizzati nello scambio di dati. HL7, definisce fondamentalmente i messaggi oggetto di scambio e più nel dettaglio definisce dei messaggi (in ASCII) e degli eventi scatenanti (trigger event o evento di trigger) che causano questi messaggi. Ad ogni messaggio dovrà corrispondere un messaggio di risposta o ACK (acknowledgment) per indicare il successo nel trasferimento delle informazioni. Ogni messaggio HL7 è composto da tanti segmenti e ogni segmento contiene un numero variabile di

campi. Ogni campo, invece, è separato dagli altri da un delimitatore chiamato separatore di campo (carattere "|") e contiene dei dati elementari detti componenti.

FHIR (Fast Healthcare Interoperability Resource) è uno standard di interoperabilità sviluppato da HL7 e progettato per consentire lo scambio di dati sanitari in formato elettronico tra sistemi diversi del settore sanitario. FHIR è la specifica più recente per la condivisione di dati e include l'esperienza e la conoscenza dei modelli logici e teorici esistenti. Di conseguenza, fornisce un'implementazione semplificata per lo scambio di dati fra applicazioni sanitarie senza sacrificarne l'integrità. È stato progettato per soddisfare la crescente complessità dei dati sanitari, le aspettative degli utenti e la necessità di un approccio moderno e basato su Internet per comunicare tra diversi componenti discreti.

FHIR ha l'obiettivo di rendere le cartelle cliniche elettroniche disponibili, individuabili e facilmente comprensibili per le parti interessate, mentre i pazienti si muovono all'interno dell'ecosistema sanitario. Questo standard non solo rende più facile per il paziente tenere traccia della propria salute, ma promuove il supporto decisionale clinico automatizzato e l'uso di altri processi basati su intelligenza artificiale o macchine. Le ragioni per cui FHIR è sempre più necessario sono molteplici:

- La tecnologia sanitaria è sempre più digitalizzata. Le cartelle cliniche elettroniche di un paziente devono essere disponibili, reperibili e comprensibili da tutti i vari operatori sanitari che il paziente vede. Lo scambio di dati sanitari è estremamente importante nel mondo connesso per rendere il sistema più efficiente ed efficace.
- Circa un terzo delle richieste di risarcimento per cattiva condotta medica sono legate a difetti di comunicazione. Ciò avviene sia tra il medico e il paziente che tra gli operatori sanitari. È fondamentale poter inviare i messaggi giusti tra le aziende del settore sanitario al momento giusto.
- L'informatica sanitaria deve sempre mettere il paziente al primo posto. L'interoperabilità è indispensabile per sviluppare un approccio orientato al paziente.

3.2.3 Standard DICOM

Lo standard DICOM [16], abbreviazione di Digital Imaging and Communication in Medicine, è il protocollo di comunicazione standard utilizzato per l'acquisizione, l'archiviazione e la trasmissione di immagini mediche e dati correlati. DICOM nell'imaging medico funge da modello per le strutture informative e le procedure che controllano l'input e l'output dei dati nei sistemi di imaging medicale. Il termine si riferisce sia al protocollo stesso che al formato di file corrispondente. Tutti i dati ottenuti nel processo di imaging medico sono memorizzati in questo formato. Senza di essa, la condivisione di informazioni tra diversi dispositivi di imaging sarebbe

notevolmente più difficile. DICOM è stato rilasciato nel 1993 da allora è stato fondamentale nello sviluppo della moderna radiologia, avendo migliorato immensamente il flusso di lavoro e la sostenibilità dei sistemi di imaging medicale consentendo ad apparecchiature, archivi digitali, workstation e server di diversi fornitori di condividere informazioni senza sforzo.

DICOM ha soddisfatto efficacemente la necessità di un formato standardizzato per il trasferimento di immagini e dati medici emersi negli anni '80, quando sono stati introdotti l'imaging medico e l'informatica nel lavoro clinico. Alcune specifiche dello standard DICOM includono:

- Formato file: DICOM utilizza un formato file basato su un formato di file universale noto come formati di file di tipo IFF;
- Struttura dati: il formato DICOM organizza i dati associati alle immagini mediche in una struttura gerarchica che comprende elementi come metadati, immagini, rapporti diagnostici e informazioni sul paziente;
- Metadati: il formato DICOM contiene una serie di metadati che descrivono le caratteristiche dell'immagine medica, come le dimensioni dell'immagine, la risoluzione, la modalità di acquisizione e le impostazioni del dispositivo di acquisizione.

L'utilizzo dello standard DICOM comporta numerosi vantaggi per la gestione e l'elaborazione delle immagini mediche. Oltre all'interoperabilità, i vantaggi portati dall'uso di questo standard sono:

- Efficienza: Lo standard DICOM semplifica la gestione e l'elaborazione delle immagini mediche, riducendo i tempi necessari per la preparazione delle immagini, la consultazione dei dati e la condivisione delle informazioni. Ciò può aumentare l'efficienza delle procedure mediche e ridurre i costi associati;
- Qualità delle immagini: Lo standard DICOM definisce una serie di specifiche per la gestione delle immagini mediche, tra cui la risoluzione, la compressione delle immagini e le impostazioni del dispositivo di acquisizione. Ciò può migliorare la qualità delle immagini mediche e garantire la loro conformità agli standard di qualità;
- Sicurezza dei dati: Lo standard DICOM include specifiche per garantire la sicurezza dei dati medici, come l'accesso autorizzato e la crittografia dei dati. Ciò può proteggere i dati medici sensibili dai rischi di accesso non autorizzato e di violazione della privacy.

4. Cenni sulle tecnologie di rete ottimali per interconnettere dispositivi medici e problematiche

4.1 Rete LAN e indirizzo IP

Una rete LAN (Local Area Network) è una rete informatica che collega i dispositivi informatici all'interno di un'area geografica limitata, come un edificio o una azienda. È progettata per facilitare la condivisione di risorse e informazioni tra i dispositivi collegati nella rete. Nelle reti LAN, i dispositivi come computer, stampanti, server, telefoni e dispositivi di rete sono collegati tra loro utilizzando cavi di rete come i cavi Ethernet. Questi dispositivi comunicano tra loro scambiandosi pacchetti di dati attraverso la rete.

Le reti LAN offrono diversi vantaggi, tra cui:

- Condivisione di risorse: I dispositivi collegati a una LAN possono condividere risorse come stampanti, file, applicazioni e connessioni Internet;
- Comunicazione: La rete LAN consente la comunicazione diretta e rapida tra i dispositivi collegati, permettendo la collaborazione e lo scambio di informazioni tra gli utenti;
- Efficienza: Con una rete LAN, i dati possono essere trasmessi tra i dispositivi a velocità elevate, consentendo il trasferimento rapido di file e l'accesso rapido alle risorse condivise.

Ogni dispositivo connesso a una rete informatica ha una etichetta univoca assegnata chiamata indirizzo IP (Internet Protocol). Ci sono principalmente due categorie di indirizzo IP:

- Indirizzo IP dinamico: È un indirizzo IP assegnato temporaneamente a un dispositivo da un server. Gli indirizzi IP dinamici possono cambiare ogni volta che il dispositivo si connette alla rete;
- Indirizzo IP statico: È un indirizzo IP fisso assegnato permanentemente a un dispositivo. Non cambia nel tempo e viene solitamente utilizzato per dispositivi che devono essere sempre accessibili tramite lo stesso indirizzo IP.

4.2 VLAN, Switch di rete e rete air-gapped

Una rete LAN può essere divisa in più VLAN in base alle necessità. Una VLAN (Virtual Local Area Network) è una tecnologia di rete che consente di creare reti logiche all'interno di una rete fisica. Una VLAN suddivide una rete locale in più segmenti virtuali, consentendo a gruppi di dispositivi di comunicare tra loro come se fossero fisicamente collegati a reti separate.

Con una VLAN, i dispositivi possono essere raggruppati in base a criteri come la posizione fisica, il reparto o la funzione. Questo permette di ottenere maggiore flessibilità nella gestione

della rete e di migliorare la sicurezza, il controllo del traffico e l'efficienza delle operazioni di rete.

Le VLAN offrono numerosi vantaggi, tra cui:

- Segmentazione della rete: Le VLAN consentono di suddividere una rete fisica in più segmenti logici indipendenti. Ciò consente di separare i dispositivi in base alle loro funzioni, dipartimenti, gruppi di lavoro o requisiti di sicurezza. La segmentazione della rete migliora la sicurezza e la gestione delle risorse;
- Sicurezza migliorata: Utilizzando le VLAN, è possibile isolare e separare i dispositivi in base alle politiche di sicurezza. Ciò impedisce ai dispositivi non autorizzati di accedere a risorse sensibili o compromettere la sicurezza del sistema. Inoltre, le VLAN possono essere utilizzate per implementare politiche di sicurezza diverse su segmenti di rete separati;
- Controllo del traffico di rete: Le VLAN consentono di gestire il traffico di rete in modo più efficiente. È possibile controllare il flusso di dati tra le VLAN attraverso regole di routing e filtri di pacchetti. Ciò consente di ottimizzare le prestazioni di rete, riducendo il carico sulle singole VLAN e migliorando la larghezza di banda disponibile per ogni segmento;
- Flessibilità nella gestione dei cambiamenti: Le VLAN semplificano la gestione delle modifiche nella rete. È possibile aggiungere, rimuovere o spostare dispositivi tra le VLAN senza dover modificare l'infrastruttura fisica della rete. Ciò consente una maggiore flessibilità nell'adattamento della rete alle esigenze aziendali in continua evoluzione;
- Aumento dell'affidabilità: Le VLAN possono migliorare l'affidabilità della rete. In caso di guasti o problemi in una VLAN specifica, le altre VLAN rimangono isolate e non vengono influenzate. Ciò consente di limitare l'impatto dei guasti e di mantenere l'integrità delle altre parti della rete.

Per consentire la comunicazione tra due VLAN, è necessario utilizzare un dispositivo di rete, come uno switch con funzionalità di routing inter-VLAN. Questi dispositivi consentono il passaggio del traffico tra le VLAN, consentendo ai dispositivi di comunicare tra loro.

Uno switch è un dispositivo di rete che consente di connettere diversi dispositivi in una rete locale (LAN) o più VLAN e di instradare il traffico di rete tra di essi. Lo switch è in grado di esaminare gli indirizzi dei pacchetti di dati e di inviarli solo al destinatario corretto, migliorando così le prestazioni e la sicurezza della rete.

Tra le principali caratteristiche degli switch di rete, ci sono:

1. Numero di porte: determina il numero di dispositivi che possono essere collegati allo switch. Gli switch possono avere un numero variabile di porte, da 4 a oltre 100.
2. Velocità della porta: indica la velocità massima di trasferimento dei dati su ogni porta dell'interruttore. Le porte possono essere di diverse velocità, come ad esempio 10/100/1000 Mbps o 10 Gbps.
3. Capacità di commutazione: indica la quantità di dati che lo switch è in grado di gestire contemporaneamente. Maggiore è la capacità di commutazione, maggiore è la quantità di dati che possono essere gestiti senza perdere prestazioni.
4. Memoria di buffering: permette di gestire i pacchetti di dati in entrata, mantenendoli in attesa fino a quando non possono essere elaborati e trasmessi al dispositivo di destinazione.
5. Sicurezza di rete: gli switch possono essere dotati di funzionalità di sicurezza avanzate, come ad esempio la gestione degli accessi basati su porte o su VLAN, la sicurezza delle porte e l'individuazione di attacchi informatici.

Tra i parametri di configurazione degli switch di rete ci sono:

1. Quality of Service (QoS): permette di definire priorità di traffico per i pacchetti di dati in modo da garantire la disponibilità di larghezza di banda per le applicazioni più critiche.
2. Port Mirroring: consente di copiare il traffico di rete da una porta dello switch ad un'altra, consentendo di monitorare il traffico della rete.
3. Aggregazione di porte: consente di combinare più porte di switch per aumentare la larghezza di banda e la ridondanza.

In generale, il traffico di rete viene instradato dal dispositivo di rete tra le VLAN utilizzando un protocollo di routing, come ad esempio il protocollo di routing IP. Quando un pacchetto di dati viene inviato da un dispositivo in una VLAN, il dispositivo di rete lo riceve e lo instrada verso la VLAN di destinazione. Il protocollo di routing IP è un protocollo di rete che consente di instradare i pacchetti di dati tra le reti interconnesse, è responsabile dell'instradamento dei pacchetti di dati tra i router della rete, in modo da garantire che i pacchetti raggiungano la loro destinazione. Senza il protocollo di routing IP, i pacchetti di dati non potrebbero essere instradati attraverso la rete e non sarebbe possibile la comunicazione tra le reti.

Tramite gli switch di rete è possibile isolare una o più VLAN, come quella degli elettromedicali o del server di archiviazioni dati (VLAN in cui sono presenti dati sensibili), creando una rete air-gapped. Una rete air-gapped è una rete informatica che è fisicamente o logicamente isolata da altre reti o risorse esterne non protette. Questa separazione viene realizzata per garantire un

elevato livello di sicurezza e protezione per le informazioni sensibili o critiche. Nel contesto di una rete air-gapped, non esiste alcuna connessione di rete diretta o accessibile dall'esterno che possa permettere il flusso di dati o comunicazioni tra la rete isolata e le reti esterne. L'obiettivo principale dell'air-gapping è prevenire la possibilità di intrusioni o attacchi informatici che potrebbero sfruttare le connessioni di rete per compromettere la sicurezza dei dati. Poiché le reti air-gapped sono isolate, i metodi tradizionali di attacco informatico, come l'accesso remoto non autorizzato o il malware che si diffonde attraverso la rete, diventano molto più difficili. Tuttavia, è importante notare che l'air-gapping non fornisce una protezione assoluta, poiché possono esistere altre potenziali vulnerabilità.

4.3 Firewall

Il firewall è un sistema di sicurezza informatica progettato per proteggere un dispositivo o una rete da attacchi esterni. Il suo ruolo principale è quello di filtrare il traffico di rete e controllare le connessioni in entrata e in uscita. Il firewall funziona come una barriera tra la rete locale e una esterna, generalmente Internet. Quando una richiesta di connessione arriva al dispositivo o alla rete, il firewall verifica se la connessione è legittima e consente o blocca l'accesso in base alle regole di sicurezza predefinite.

I vantaggi di utilizzare un firewall sono diversi:

- Sicurezza della rete: Il firewall protegge la rete interna filtrando il traffico indesiderato o pericoloso proveniente da Internet. Blocca tentativi di intrusioni e attacchi informatici, come malware, virus, worm e tentativi di hacking;
- Controllo degli accessi: Il firewall offre la possibilità di definire regole di accesso che determinano quali tipi di traffico e quali servizi possono essere acceduti dalla rete interna e quali devono essere bloccati. Ciò consente di controllare e limitare l'accesso a determinati siti web, protocolli o servizi che potrebbero rappresentare un rischio per la sicurezza o consumare risorse di rete inutilmente;
- Protezione dei dati sensibili: Un firewall può impedire che informazioni sensibili o riservate lascino la rete interna senza autorizzazione. Può monitorare il traffico in uscita e applicare regole per bloccare il trasferimento di dati confidenziali o critici;
- Filtraggio del contenuto: I firewall possono implementare filtri per bloccare o limitare l'accesso a determinati tipi di contenuti web, come siti web inappropriati, social media o servizi di file sharing. Ciò aiuta a mantenere un ambiente di lavoro produttivo e può ridurre i rischi derivanti da contenuti potenzialmente dannosi o non sicuri;
- Monitoraggio e registrazione: I firewall offrono funzionalità di monitoraggio in tempo reale del traffico di rete e possono generare registri dettagliati degli eventi. Questo

consente agli amministratori di rete di identificare potenziali minacce, analizzare incidenti di sicurezza e monitorare l'utilizzo della rete.

Inoltre, il firewall può essere usato anche come 'filtro' fra le VLAN. Un firewall può essere configurato per consentire o bloccare il traffico tra le VLAN in base a determinate regole di sicurezza. Ad esempio, è possibile definire regole che consentono il flusso di dati solo tra specifiche VLAN o limitare l'accesso a determinati servizi o risorse solo a VLAN specifiche. Utilizzando un firewall per gestire il traffico tra VLAN, è possibile aumentare la sicurezza della rete, controllare l'accesso tra segmenti di rete diversi e impedire che minacce o attività non autorizzate si diffondano tra le VLAN. Ciò consente una maggiore segmentazione e controllo del traffico all'interno della rete, migliorando la sicurezza complessiva e ottimizzando le prestazioni della rete.

4.4 Connessione RD e VPN

Una connessione RD (Remote Desktop) è una tecnologia che consente a un utente di accedere e controllare un computer da remoto o, come in questo caso, un server da un altro dispositivo tramite una rete. Attraverso una connessione RD, è possibile visualizzare l'interfaccia del sistema operativo del server e interagire con esso come se si fosse fisicamente davanti a esso. Questo può essere utile per gestire e amministrare il server da remoto, installare software, configurare impostazioni o accedere alle risorse e ai file presenti sul server. È importante notare che la connessione RD al server richiede le necessarie autorizzazioni e credenziali di accesso

Inoltre, è importante considerare la sicurezza della connessione RD, ad esempio utilizzando crittografia e misure di autenticazione forti, per proteggere l'accesso e le informazioni sensibili sul server durante la connessione remota. Per aumentare la sicurezza della connessione RD viene usata una VPN. Una VPN (Virtual Private Network) crea un tunnel crittografato tra il tuo dispositivo e il server VPN, rendendo più difficile per gli attaccanti intercettare o manipolare i tuoi dati durante il trasferimento attraverso Internet. Usare una VPN offre i seguenti vantaggi:

- Crittografia dei dati: Una VPN crittografa i dati che invii e ricevi durante la connessione. Questo significa che anche se qualcuno riesce ad intercettare i tuoi dati, non sarà in grado di leggerli o interpretarli senza la chiave di decrittografia corretta.
- Protezione delle informazioni personali: Utilizzando una VPN, puoi nascondere il tuo indirizzo IP e la tua posizione fisica. Questo rende più difficile per le organizzazioni o gli individui monitorare le tue attività online, migliorando così la tua privacy.

Nonostante i benefici, è importante ricordare che una VPN non fornisce una sicurezza totale in quanto, per esempio, il protocollo di comunicazione potrebbe avere delle vulnerabilità nella sua implementazione consentendo ad utenti non autorizzati di intercettare i dati.

4.5 Hardening dei sistemi

Per Hardening dei sistemi si intende l'insieme di strumenti, metodi e procedure consigliate impiegati per ridurre la superficie di attacco nell'infrastruttura tecnologica, compresi software, sistemi di dati e hardware. L'obiettivo dell'Hardening dei sistemi è ridurre il "profilo delle minacce" complessivo o le aree vulnerabili del sistema. L'Hardening dei sistemi implica il controllo metodico, l'identificazione e la correzione di potenziali vulnerabilità di sicurezza all'interno di un'intera organizzazione, spesso con particolare attenzione alla regolazione delle varie impostazioni e configurazioni predefinite per renderle più sicure. L'obiettivo del rafforzamento dei sistemi è ridurre quanto più possibile i rischi per la sicurezza. Riducendo al minimo la superficie di attacco, i malintenzionati hanno meno mezzi di accesso o potenziali punti di appoggio per iniziare un attacco informatico. Per superficie di attacco si intende la combinazione di tutti i potenziali difetti nella tecnologia che potrebbero essere sfruttati. In genere, queste vulnerabilità comprendono:

- Password o credenziali predefinite memorizzate in file accessibili;
- Software privi di patch;
- Dati non crittografati;
- Dispositivi dell'infrastruttura mal configurati;
- Impossibilità di impostare correttamente le autorizzazioni degli utenti;
- Errata configurazione degli strumenti di sicurezza informatica.

L'Hardening dei sistemi è un'attività essenziale per la sicurezza e la conformità, oltre a costituire una parte cruciale di una più ampia strategia di sicurezza delle informazioni. Il vantaggio più evidente del rafforzamento dei sistemi è la riduzione del rischio di attacchi informatici e dei relativi tempi di inattività e sanzioni normative.

5. Caso di studio: messa in rete di un sistema cardiotocografico presso l'AULSS4

5.1 Il caso di studio

Un sistema di monitoraggio cardiotocografico è un dispositivo medico utilizzato per monitorare la salute fetale durante la gravidanza e il parto. La cardiotocografia (CTG) è un esame non invasivo, molto diffuso in ostetricia, che si effettua dalla 27ª settimana di gravidanza per valutare alcuni fattori importanti:

- Indagare il benessere fetale attraverso lo studio del battito cardiaco;
- Rilevare la presenza o l'assenza delle contrazioni uterine e la loro frequenza;
- In fase di travaglio per valutare se è necessario accelerare il parto o procedere con il cesareo.

In particolare, il monitoraggio CTG può rivelare eventuali anomalie nella frequenza cardiaca fetale, come bradicardia o tachicardia, che potrebbero indicare un insufficiente apporto di ossigeno al feto. Il monitoraggio CTG può anche aiutare a identificare eventuali complicazioni del parto, come l'arrotondamento del cordone ombelicale, che potrebbe mettere a rischio la vita del feto. L'esame è stato introdotto in Italia negli anni Settanta con lo scopo di ridurre la mortalità perinatale (termine che comprende tutte le morti che avvengono tra la 27ª settimana di gravidanza e la prima settimana di vita extrauterina).

Il sistema di monitoraggio CTG si compone di due sensori posti sull'addome della madre: uno rileva l'attività elettrica del cuore fetale attraverso un trasduttore ad ultrasuoni, mentre l'altro rileva le contrazioni uterine tramite un trasduttore di pressione. I segnali raccolti dai sensori sono poi visualizzati su un grafico, che può essere letto dal medico o dal personale medico.

5.2 Composizione del sistema di monitoraggio

Il sistema di monitoraggio fetale oggetto del piano di messa in rete è composto così come segue:

- U.O.C. Ostetricia Ginecologia San Donà di Piave:
    - n. 6 Monitor fetale cardiotocografico (Monitor fetale Philips Avalon FM30)
    - n. 4 Sistema telemetrico per monitoraggio fetale cardiotocografico (Sistema Telemetrico Cableless- Philips Avalon CL)
    - n. 1 Centrale di monitoraggio (Philips IntelliSpace Perinatal)
    - n. 1 Server di archiviazione dati (HP Proliant mod. DL360)
- U.O.C. Ostetricia Ginecologia Portogruaro:
    - n. 4 Monitor fetale cardiotocografico (Monitor fetale Philips Avalon FM30)

- n. 2 Sistema telemetrico per monitoraggio fetale cardiotocografico (Sistema Telemetrico Cableless- Philips Avalon CL)
- n. 1 Centrale di monitoraggio (Philips IntelliSpace Perinatal)

Per un totale di:
-n. 10 monitor fetale cardiotocografico
-n. 6 sistema telemetrico per monitoraggio fetale cardiotocografico
-n. 2 centrale di monitoraggio
-n. 1 server di archiviazione
Inoltre, ogni postazione per il monitoraggio comprende una stampante.

5.3 Caratteristiche del sistema di monitoraggio

- Monitor fetale Philips Avalon FM30 [17]: Il monitor fetale Philips Avalon FM30 è un dispositivo medico utilizzato per il monitoraggio continuo del battito cardiaco fetale e delle contrazioni uterine durante la gravidanza e il parto. È progettato per fornire un'accurata valutazione dello stato del feto e della madre durante il travaglio e il parto, consentendo ai professionisti sanitari di prendere decisioni informate e tempestive per garantire la sicurezza del bambino e della madre. Il monitor fetale Avalon FM30 è dotato di una tecnologia avanzata che permette una rilevazione precisa e affidabile dei segnali vitali. Utilizza sonde ad ultrasuoni per monitorare il battito cardiaco fetale e un sensore per registrare le contrazioni uterine. I dati raccolti vengono visualizzati su un display chiaro e intuitivo, che consente ai medici e agli operatori sanitari di valutare facilmente i parametri vitali del bambino e della madre. Una delle caratteristiche distintive dell'Avalon FM30 è la sua capacità di connessione wireless. Il monitor può essere collegato a una rete di monitoraggio centrale che consente al personale medico di monitorare i segnali vitali del feto e della madre da un'unica postazione o tramite dispositivi mobili come smartphone o tablet. Questa caratteristica favorisce la mobilità e la flessibilità durante il travaglio e il parto, consentendo ai medici di monitorare attentamente i pazienti anche durante gli spostamenti. Il monitor Avalon FM30 rileva e documenta:
  - Fino a tre frequenze cardiache fetali con il monitoraggio esterno a ultrasuoni;
  - Il monitoraggio della frequenza cardiaca fetale con ECG fetale diretto (DECG), inclusa visualizzazione della forma d'onda;
  - L’attività uterina con trasduttore toco (monitoraggio esterno) oppure con la pressione intrauterina (IUP);

- La frequenza cardiaca materna con visualizzazione della forma d'onda ECG;
- La SpO2 materna (pulsossimetria) e la pressione sanguigna materna non invasiva.

- Sistema Telemetrico Cableless (Wireless) - Philips Avalon CL [18]: Il Sistema di Trasduttori Cableless Avalon CL rileva e trasmette via radio i parametri fetali standard a un monitor fetale compatibile, eliminando così i cavi di collegamento dei Trasduttori. Assicura la massima flessibilità, eliminando i cavi per tutte le misurazioni dei parametri fetali e materni possibili. Il sistema è stato progettato per l'uso nel periodo prenatale, durante il travaglio e il parto.
- Centrale di monitoraggio con software 'Philips IntelliSpace Perinatal' [19]: Il sistema di gestione Philips "IntelliSpace Perinatal" con funzione di sorveglianza, allarme, memorizzazione e documentazione completa dei dati delle pazienti, è in grado di fornire tutte le informazioni necessarie a documentare e gestire il percorso terapeutico nel reparto di Ostetricia. Il sistema è basato su standard industriali, con architettura client/server di Microsoft Windows e un'interfaccia utente mentre si connetterà al server virtuale e al server di archiviazione tramite connessione da remoto RDP. Il sistema di monitoraggio comprende:
  - Il Sistema Intellispace Perinatal
  - L'hardware include una workstation basata su PC desktop (HP Elite Desk705, CPU: Ryzen 5 PRO, RAM: 8 GB, HD: 256 GB SSD) avente mouse, tastiera, adattatore di rete, scheda grafica integrata, unità CD ROM/DVD Drive, disco SSD, scheda audio, licenza software per memorizzazione su NAS (Network Area Storage) e display da 27".

  Il software Philips "IntelliSpace Perinatal" adotta come protocollo di comunicazione lo standard HL7.
- Server di archiviazione dati HP Proliant mod. DL360: Server per l'archiviazione dei dati di entrambi i sistemi, presenti a San Donà di Piave e Portogruaro, dotato di dispositivi di sicurezza per la salvaguardia dei dati memorizzati e con sistema di back up che consente il ripristino dei dati. Il server è costituito da 2 dischi in configurazione con una capacità di memoria complessiva pari a 1,2 TB. Le Centrali di monitoraggio avranno il pieno accesso al server memorizzando i dati paziente e con piena possibilità di interrogazione dello storico.

5.4 Composizione della rete ospedaliera

Tutti i dispositivi, che compongono il sistema di monitoraggio fetale, precedentemente elencati e descritti saranno collegati alla rete ospedaliera così:

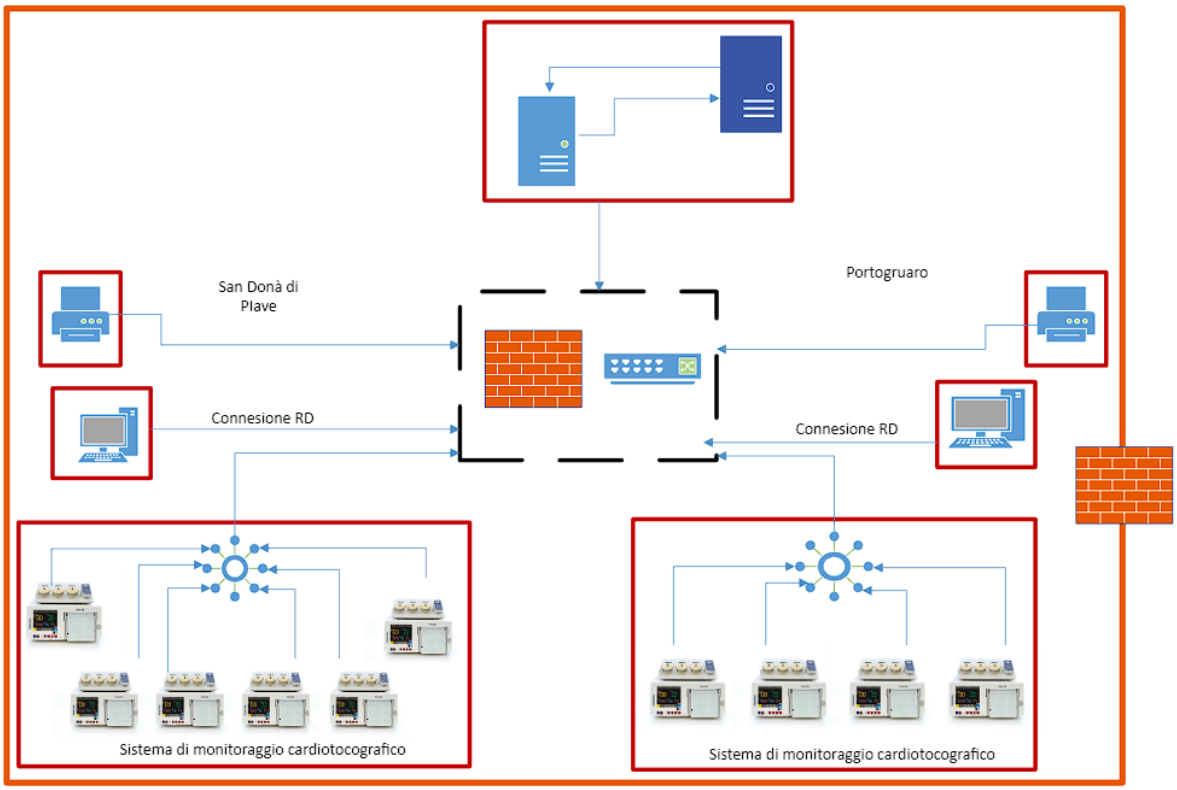

Fig. 2: Schema della messa in rete del sistema cardiotocografico

Fig3: Leggenda

5.4.1 Rete LAN presso l'AULSS4

Ogni ospedale dell'AULSS4 ha una propria rete LAN. Nel caso in esame verranno prese in considerazione le reti LAN dell'ospedale di San Donà di Piave e di Portogruaro. Ogni dispositivo avrà un proprio indirizzo IP statico come per tutti i dispositivi connessi alla rete ospedaliera.

5.4.2 VLAN e Switch di rete presso l'AULSS4

Negli ospedali presi in considerazione la rete ospedaliera è divisa così come segue:

- Ospedale di San Donà di Piave: attualmente la rete ospedaliera è divisa nelle seguenti VLAN:
    - VLAN per controllo accessi
    - VLAN per le workstation
    - VLAN per la telefonia
    - VLAN per le stampanti
    - VLAN per gli elettromedicali
    - VLAN server
- Ospedale di Portogruaro: attualmente la rete ospedaliera è divisa nelle seguenti VLAN:
    - VLAN per controllo accessi
    - VLAN per le workstation
    - VLAN per la telefonia
    - VLAN per le stampanti
    - VLAN per gli elettromedicali
    - VLAN server

L'AULSS4 ha in programma un piano di ampliamento delle VLAN attualmente esistenti. In particolare, si prevede di arrivare ad avere le seguenti VLAN:

- VLAN per i server
- VLAN per controllo accessi
- VLAN per i computer
- VLAN per la telefonia
- VLAN per le stampanti
- VLAN per gli elettromedicali diagnostici
- VLAN per la strumentazione degli elettromedicali
- VLAN per le workstation elettromedicali

Sono previste altre VLAN ma non sono di interesse per il caso preso in esame.

Attualmente l'AULSS4 ha in dotazione, presso le proprie sedi ospedaliere, due tipo di switch di rete con le seguenti caratteristiche:

- HPE Aruba 2930M 48G PoE+ Switch (JL322AC) [20]:
    - Numero di porte: Lo switch dispone di 48 porte Gigabit Ethernet
    - Velocità delle porte: Le porte possono arrivare fino a 100Gb

- Capacità di commutazione: Lo switch ha una capacità massima di commutazione di 176 Gbps, consentendo una trasmissione dati ad alta velocità all'interno della rete.
- Memoria di buffering: Lo switch dispone di una memoria di buffer di 12 MB.

- HPE ARUBA 5945 2-slot (JQ075AC) [21]:
  - Numero di porte: Lo switch dispone di 48 porte Gigabit Ethernet
  - Velocità delle porte: Le porte possono arrivare fino a 100Gb
  - Capacità di commutazione: Lo switch ha una capacità massima di commutazione di 3.6 Tb/s, consentendo una trasmissione dati ad alta velocità all'interno della rete.
  - Memoria di buffering: Lo switch dispone di una memoria di buffer di 32 MB.

5.4.3 **Firewall presso l'AULSS4**

L'ULSS4 attualmente dispone di un firewall perimetrale che filtra tutti gli accessi che provengono dall'esterno della rete ospedaliera e una serie di firewall interni che gestiscono le autorizzazioni a comunicare o meno fra dispositivi di diverse VLAN. Quindi, un utente esterno alla rete ospedaliera non potrà accedere a quest'ultima senza le necessarie autorizzazioni come, un utente all'interno della rete ospedaliera non potrà accedere a VLAN a cui non è autorizzato ad accedere.

5.4.4 **Connessione RD e VPN presso l'AULSS4**

Il server fisico di archiviazione e il server IntelliSpace perinatal sono entrambi installati presso il data center presente all'ospedale di San Donà di Piave. Le due centrali di monitoraggio accederanno al server IntelliSpace perinatal e al server fisico di archiviazione tramite connessione RD. La connessione RD al server richiede le necessarie autorizzazioni e credenziali di accesso che, in AULSS4 sono gestite dai 'Sistemi Informativi' presso l'Ospedale di San Donà di Piave. Inoltre, per aumentare la sicurezza della connessione RD viene usata una VPN.

5.5 Mitigazione del rischio rispetto a una rete piatta

Una rete piatta è un'architettura di rete in cui tutti i dispositivi connessi condividono lo stesso livello di autorizzazione e accesso alla rete. In una rete piatta, non sono presenti segmentazioni o divisioni gerarchiche tra i dispositivi connessi. Una rete piatta è generalmente considerata meno sicura rispetto a una rete segmentata o gerarchica. Ciò è dovuto al fatto che in una rete piatta, tutti i dispositivi connessi condividono lo stesso livello di autorizzazione e accesso alla

rete, senza restrizioni o misure di sicurezza che limitano l'accesso a parti specifiche della rete. Le ragioni per cui una rete piatta è considerata non sicura sono:

- Maggior esposizione alle vulnerabilità: Con una rete piatta, i dispositivi potrebbero essere più esposti a minacce come attacchi di rete, malware, phishing e altre forme di attacchi informatici. Poiché tutti i dispositivi sono accessibili sulla stessa rete, una vulnerabilità su uno di essi potrebbe potenzialmente compromettere tutti gli altri dispositivi;
- Diffusione di attacchi: Se un dispositivo in una rete piatta venisse compromesso, l'attaccante potrebbe potenzialmente accedere e compromettere tutti gli altri dispositivi connessi alla stessa rete. La mancanza di segmentazione impedisce di limitare la diffusione di un attacco a una parte specifica della rete;
- Accesso non autorizzato: In una rete piatta, tutti i dispositivi possono comunicare tra loro senza restrizioni. Ciò significa che un dispositivo non autorizzato o un utente malintenzionato potrebbe accedere e interagire con dispositivi sensibili o risorse critiche all'interno della rete.

Rispetto a una rete piatta le reti ospedaliere analizzate garantiscono:

- Segmentazione della rete grazie all'uso delle VLAN;
- Autorizzazione degli accessi gestiti dai Sistemi Informativi;
- Filtrazione degli accessi grazie all'uso dei firewall;
- Crittografia dei dati grazie all'utilizzo della VPN.

Le reti ospedaliere in analisi offrono un buon livello di sicurezza e possono quindi, essere considerate più sicure di una rete piatta.

5.6 DPIA per il sistema di monitoraggio cardiotocografico

Trattando dati personali sensibili in ambiente sanitario, il GDPR richiede che venga redatto obbligatoriamente il DPIA per il sistema di monitoraggio cardiotocografico. I 'Sistemi Informativi' dell'AULSS4 dispongono di una piattaforma apposita per la compilazione del DPIA. In particolare, le informazioni principali richieste sono:

- Descrizione del trattamento dei dati: Si spiega nel dettaglio il tipo di dati personali che saranno trattati, la finalità del trattamento e come verranno raccolti, utilizzati, conservati e trasferiti;
- Valutazione della necessità e della proporzionalità: Si spiega perché è necessario trattare i dati personali e se ci sono alternative meno invasive. Inoltre, bisogna assicurarsi che il trattamento sia proporzionato agli obiettivi che si intendono raggiungere;

- Valutazione dei rischi per i diritti e le libertà degli interessati: Vengono identificati e valutati i rischi che potrebbero derivare dal trattamento dei dati, come la perdita, l'accesso non autorizzato, la divulgazione, l'alterazione o la distruzione dei dati;
- Misure di mitigazione dei rischi: Vengono descritte le misure tecniche e organizzative che saranno implementate per ridurre i rischi identificati. Ciò include l'adozione di misure di sicurezza, l'implementazione di procedure di gestione dei dati e la formazione del personale.

CONCLUSIONI

La messa in rete dei dispositivi medici ha aperto nuove possibilità nella gestione dei dati e nella fornitura di cure mediche, ma ha anche presentato una serie di sfide significative che richiedono attenzione e soluzioni efficaci. Si è evidenziato l'importanza delle normative per garantire la sicurezza dei dispositivi medici e la sicurezza informatica delle reti ospedaliere. Le normative future dovranno tener conto delle sfide sempre maggiori per garantire la sicurezza dei dati e delle comunicazioni. È fondamentale che i regolamenti promuovano una collaborazione efficace tra gli sviluppatori, i fornitori di dispositivi medici e le istituzioni di regolamentazione al fine di garantire standard di sicurezza elevati e una corretta implementazione delle tecnologie di rete.

Inoltre, le problematiche di interoperabilità rappresentano un ostacolo significativo che richiede l'adozione di standard comuni per la comunicazione e lo scambio di dati tra i dispositivi medici. L'assenza di standard può limitare la capacità dei dispositivi di lavorare in modo sinergico, ostacolando l'efficacia del sistema sanitario stesso e quindi, non garantendo una cura efficace al paziente. Pertanto, gli sforzi per adottare standard interoperabili devono essere incentivati e supportati.

La sicurezza dei dispositivi medici collegati in rete è una priorità fondamentale. La protezione dei dati, la prevenzione degli accessi non autorizzati e la mitigazione dei rischi legati alle minacce informatiche sono elementi essenziali per garantire la sicurezza dei pazienti. È necessario adottare approcci multistrato che includano la crittografia, l'autenticazione forte e i meccanismi di monitoraggio per identificare e rispondere rapidamente alle potenziali violazioni della sicurezza.

Quindi, la messa in rete dei dispositivi medici offre opportunità significative per migliorare l'assistenza sanitaria, ma richiede un approccio globale che consideri attentamente le normative, le problematiche di interoperabilità e la sicurezza. Le istituzioni di regolamentazione, gli sviluppatori e i fornitori di dispositivi medici devono collaborare per sviluppare standard comuni, migliorare l'interoperabilità e garantire la sicurezza dei dispositivi medici connessi in una rete. Solo attraverso un approccio integrato e la consapevolezza delle sfide presenti, sarà possibile massimizzare i benefici offerti dalla messa in rete dei dispositivi medici e garantire cure di alta qualità e sicurezza per i pazienti.

Per quanto riguarda la messa in rete del sistema cardiotocografico illustrato nell'elaborato, la struttura della rete presente negli ospedali dell'AULSS4 in esame garantisce un buon livello di sicurezza potendo contare su una segmentazione della rete tramite VLAN, su un controllo degli accessi e un'autenticazione forte oltre che a una serie di firewall con il compito di filtrare gli accessi provenienti da utenti non autorizzati esterni. È importante considerare anche le linee

guida e i requisiti specifici forniti dai produttori dei dispositivi medici e dalle autorità regolatorie competenti per garantire una gestione sicura ed efficace del sistema di monitoraggio, ma in generale di tutti i dispositivi medici. Per aumentare la sicurezza della rete si potrebbe per esempio, segmentare ulteriormente la rete ospedaliera creando delle VLAN specifiche per ogni reparto ospedaliero con relativi dispositivi medici. In questo modo, in caso di attacco hacker, si riuscirebbe a limitare l'attacco a un solo reparto e non all'intero ospedale. Ovviamente, aumentare la sicurezza di una rete informatica comporta un costo a livello economico non indifferente che in un settore, quello sanitario, è un fattore da non sottovalutare a causa dei continui tagli alla sanità.

Bibliografia

1. Rapporto Clusit sulla sicurezza ICT in italia: https://web.uniroma1.it/infosapienza/sites/default/files/RapportoClusit2019.pdf
2. Studio Daniel Halperin et al.: https://ieeexplore.ieee.org/document/4531149
3. Definizione dispositivo medico: https://www.gazzettaufficiale.it/eli/id/1997/03/06/097G0076/sg
4. MDR: https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32017R0745&from=IT
5. IVDR: https://www.gazzettaufficiale.it/eli/id/2022/09/13/22G00146/sg
6. GDPR: https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=OJ%3AL%3A2016%3A119%3AFULL
7. NIS: https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32016L1148
8. Ministero della salute: https://www.salute.gov.it/portale/ministro/p4_11.jsp?lingua=italiano&menu=organizzazione&label=nis&id=1352#:~:text=Le%20Linee%20guida%20per%20gli,reti%20e%20dei%20sistemi%20informativi
9. Framework nazionale sulla cybersecurity: https://www.cybersecurityframework.it/
10. NIS 2: https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32022L2555
11. NIST: https://www.nist.gov/cyberframework
12. IEC 80001: https://www.iso.org/obp/ui/en/#iso:std:iec:80001:-1:ed-2:v1:en,fr
13. ICD9-CM: https://www.salute.gov.it/portale/temi/p2_6.jsp?id=1278&area=ricoveriOspedalieri&menu=cl
14. HL7: https://www.hl7.org/
15. FHIR: https://www.hl7.org/fhir/
16. DICOM: https://www.dicomstandard.org/
17. Monitor fetale Philips Avalon FM30: https://www.philips.it/healthcare/product/HC862199/monitor-fetale-avalon-fm30
18. Sistema Telemetrico Cableless (Wireless) - Philips Avalon CL: https://www.philips.it/healthcare/product/HC866074/avalon-cl-sistema-di-monitoraggio-fetale-cableless
19. Intellispace perinatal: https://www.philips.it/healthcare/product/HCNOCTN177/intellispace-perinatal-sistema-di-gestione-dei-dati-di-ostetricia
20. Switch Aruba 2930M 48G PoE+ 1 slot: https://buy.hpe.com/it/it/networking/switches/fixed-port-l3-managed-ethernet-switches/2930-switch-products/switch-aruba-2930m-48g-poe-1-slot/p/jl322a
21. Switch a 2 slot HPE FlexFabric 5945: https://buy.hpe.com/it/it/networking/switches/fixed-port-l3-managed-ethernet-switches/5900-switch-products/switch-a-2-slot-hpe-flexfabric-5945/p/jq075a