CYBERSECURITY E PRIVACY RISK NELLA TELEMEDICINA

Inclusi quelli derivanti dalla Biometria, dal Cloud e dall'IoT

Autore: Aldo Pedico – Enterprise Security & Privacy

Contatto: pedicoaldo@gmail.com

PREMESSA

Tra i sistemi, gli apparati e gli ambienti in uso nella Telemedicina vanno considerati la Biometria, il Cloud e l'IoT, per cui è necessario analizzare anche i rischi derivanti dall'uso di questi sistemi.

Per affrontare i rischi relativi alla Cybersecurity e alla Privacy nella architettura della Telemedicina è necessario considerare anche le azioni problematiche derivanti dall'uso dei sistemi che compongono l'intera architettura e che sono necessari a eseguire le interazioni tra il Paziente e le Organizzazioni di Assistenza Sanitaria (HEALTHCARE DELIVERY ORGANIZATIONS – HDO).

Per permettere questa interazione, è necessario avere all'interno della struttura tecnologica una serie di apparati e ambienti, i quali aumentano i fattori di rischio da prendere in considerazione nella fase di RISK ASSESSMENT *necessaria a tutelare sia la privacy del paziente sia l'intero sistema di gestione delle informazioni.*

SCOPO

Scopo di questo articolo è di fornire degli spunti per identificare e mitigare i rischi per la sicurezza informatica e per la privacy basati sull'uso, da parte dei pazienti, di dispositivi domestici intelligenti che si interfacciano con i sistemi informativi dei pazienti stessi.

Inoltre, al fine di evidenziare una contromisura ad una potenziale vulnerabilità della Cibersicurezza e della Privacy è stato introdotto un capitolo su ZERO TRUST, *all'interno del quale si descrivono brevemente soluzioni.*

INDICE DEGLI ARGOMENTI

Titolo_____ Pag.

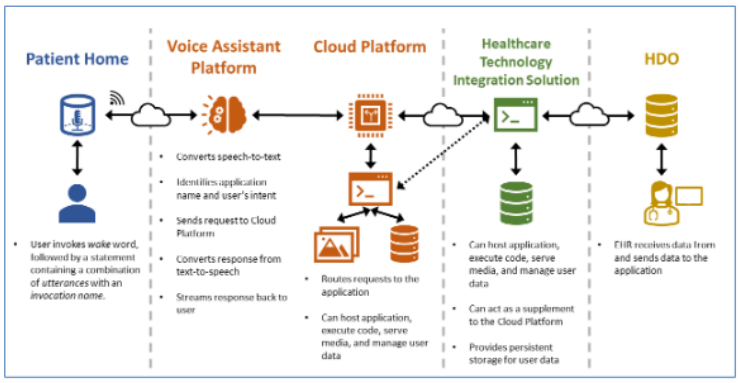
1. ANALISI DEL CONTESTO 3
1.1 Architettura generale 3
1.2 Componenti dell'architettura dei domini 3
1.3 Vista a strati dell'architettura 4
1.4 Esempio dettagliato dell'architettura Patient Home 5
1.5 Scenari 5
2. MINACCE 7
2.1 Minacce - Casa del paziente 7
2.2 Minacce - Telehealth Platform Provider 9
3. VULNERABILITÀ 10
4. AZIONI SFAVOREVOLI 11
5. RISCHI 11
6. ZERO TRUST 13
7. RIFERIMENTI 15

1. ANALISI DEL CONTESTO

1.1 ARCHITETTURA GENERALE

La Figura 3-1 descrive i presupposti dell'architettura di alto livello per quattro domini in cui i componenti operano per consentire l'integrazione della casa intelligente di telemedicina.

Figure 3-1 High-Level Architecture



1° Dominio: PATIENT HOME ENVIRONMENT.

2° Dominio: CLOUD SERVICE PROVIDER ENVIRONMENT.
Il fornitore di servizi cloud dispone di una piattaforma di assistente vocale che riceve input vocali da dispositivi domestici intelligenti e utilizza la tecnologia di elaborazione del linguaggio naturale per utilizzare l'input vocale come interfaccia utente per la logica dell'applicazione.

3° Dominio: HEALTHCARE TECHNOLOGY INTEGRATION SOLUTION.
Potrebbe esistere una logica applicativa che non richiede l'implementazione del terzo dominio. Ad esempio, può esistere una logica applicativa che consenta ai pazienti di interrogare archivi di dati generici che forniscono informazioni pubblicamente disponibili.

4° Dominio: HDO (HEALTHCARE DELIVERY ORGANIZATIONS) ENVIRONMENT.
Essi possono ospitare informazioni sui pazienti e sistemi clinici, portali per i pazienti, sistemi di registrazione elettronica o altri sistemi.

1.2 COMPONENTI DELL'ARCHITETTURA DEI DOMINI

Di seguito sono indicate le componenti dei singoli domini precedentemente descritti.

1° Dominio: COMPONENTI PER L'AMBIENTE DOMESTICO DEL PAZIENTE

- ✓ *Dispositivi Biometrici: sensore che si interfaccia con il paziente e acquisisce i dati biometrici che vengono trasmessi al medico. (vedi Table C-9 e C-10 dell'Appendix C del NIST SP 1800-30).*
- ✓ *Dispositivi con capacità di input e output audio tali da accettare comandi vocali che consentano all'utente di accedere alle risorse ospitate su Internet.*
- ✓ *Firewall personale che controlli il traffico di rete, consentendo o negando le comunicazioni in base a una politica di sicurezza.*
- ✓ *Router che includa le funzioni di un punto di accesso wireless.*

2° Dominio: AMBIENTE DEL PROVIDER DI SERVIZI CLOUD

- ✓ *Piattaforma di assistenza vocale che consenta al fornitore di servizi cloud e ad altre organizzazioni di sviluppare applicazioni che funzionino con dispositivi domestici intelligenti.*

- ✓ *Piattaforma cloud in cui le applicazioni abilitate alla voce possano essere ospitate e rese disponibili per l'interazione dei pazienti. I pazienti consentiranno alle applicazioni di telemedicina di funzionare sul proprio dispositivo intelligente.*

3° Dominio: SOLUZIONE DI INTEGRAZIONE DELLA TECNOLOGIA SANITARIA

- ✓ *Applicazioni per l'integrazione della telemedicina: codice e applicazioni che consentano alle funzionalità guidate dal paziente di interfacciarsi con i sistemi clinici.*

4° Dominio: COMPONENTI PER L'AMBIENTE HDO

- ✓ *Sistema di cartelle cliniche elettroniche* (ELECTRONIC HEALTH RECORD - EHR) *che includa informazioni sull'anamnesi sanitaria del paziente.*
- ✓ *Portale del paziente: applicazione che consenta al paziente di recuperare le informazioni sulla propria storia medica, programmare le visite e richiedere ricariche di prescrizione. Il sistema può essere distribuito nell'HDO o in un ambiente cloud/di terze parti.* L'HDO sarebbe responsabile delle funzioni di sistema indipendentemente dalla distribuzione.
- ✓ *Controllo dell'accesso alla rete per rilevare e identificare con precisione i dispositivi collegati a reti cablate, reti wireless e VPN e fornire controlli sull'accesso alla rete per garantire che solo le persone autorizzate con dispositivi autorizzati possano accedere ai sistemi e ai dati consentiti dalle policy di accesso.*
- ✓ *Firewall di rete per monitorare e controllare il traffico di rete in entrata e in uscita, in base a regole di sicurezza definite.*
- ✓ *VPN per un accesso remoto sicuro agli endpoint tramite reti private virtuali.*

1.3 VISTA A STRATI DELL'ARCHITETTURA

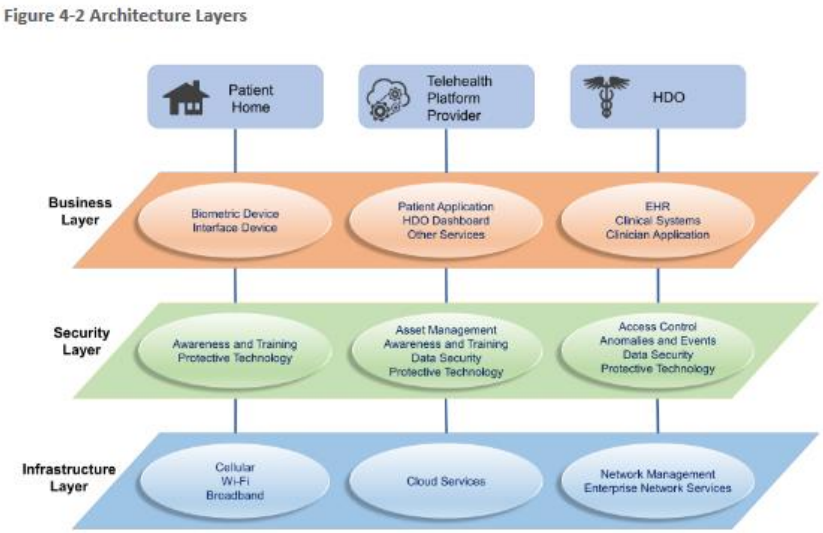
ESEMPIO: *Il laboratorio sanitario NCCoE ha stratificato l'architettura distribuita con tre livelli:*

1) BUSINESS;

2) SECURITY;

3) INFRASTRUCTURE.

(vedi figura accanto)



Il livello BUSINESS *si concentra sulle capacità funzionali che includono letture biometriche e interazioni con i pazienti. È costituito da servizi che facilitano la gestione dei dati dei pazienti e funzionalità web o di audioconferenza.*

Il livello SECURITY *descrive concettualmente come il laboratorio NCCoE implementa le funzionalità di sicurezza. È costituito da componenti utilizzati per proteggere l'ambiente, come meccanismi di*

autenticazione, sistemi di gestione dei certificati, funzionalità di registrazione della sicurezza e da componenti di rete e server che possono essere implementati come servizi cloud.

Il livello INFRASTRUCTURE *rappresenta la rete e l'ambiente di comunicazione.*

Gli strati intersecano ciascuno dei tre domini.

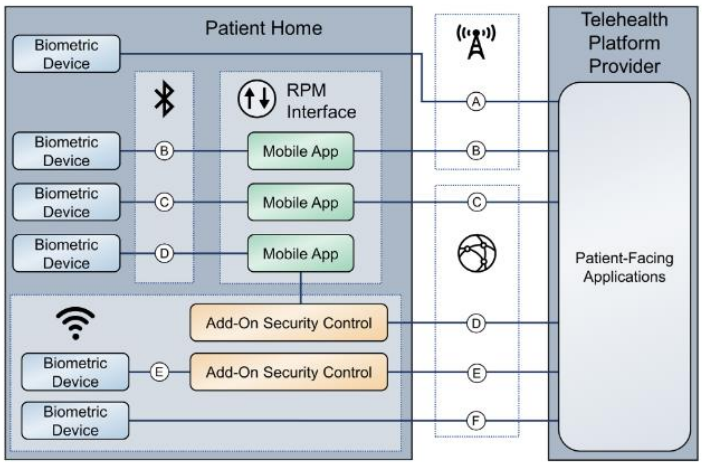
Il dominio PATIENT HOME *implementa il livello* BUSINESS *utilizzando i dispositivi biometrici e i dispositivi di interfaccia che acquisiscono e trasmettono i dati biometrici dal paziente e consentono rispettivamente al paziente di comunicare con il team di assistenza clinica.*

Il dominio HDO *implementa il livello* BUSINESS *con applicazioni e sistemi clinici utilizzati per supportare il programma* RPM *e implementa il livello* INFRASTRUCTURE *con servizi IT fondamentali come AD, DNS e dispositivi di rete.*

1.4 ESEMPIO DETTAGLIATO DELL'ARCHITETTURA PATIENT HOME

Un esempio un po' più dettagliato del protocollo di comunicazione è rappresentato nella figura 2-1 (capitolo 2.1 del NIST SP 1800-30C*) qui accanto. (Una descrizione dettagliata di ciascun percorso di comunicazione è fornita in* NIST SP 1800-30B*, Sezione 4.2, Percorsi di comunicazione di architettura di alto livello)*

Figure 2-1 RPM Communications Paths



Il Telehealth Platform Provider è terza parte che ha configurato, distribuito e gestito i dispositivi biometrici e i mobili (ad es. tablet) che sono stati inviati a casa del paziente. Inoltre, ha implementato sia un'applicazione che ha consentito ai medici di accedere ai dati biometrici sia dei dispositivi biometrici abilitati con la tecnologia wireless Bluetooth.

Questi dispositivi trasmettevano dati biometrici alla piattaforma di telemedicina basata su cloud.

Il paziente ha trasmesso i dati biometrici al fornitore della piattaforma di telemedicina utilizzando il dispositivo di interfaccia, il quale trasmetteva dati su comunicazioni dati cellulari o a banda larga.

Il fornitore di piattaforme di telemedicina ha consentito agli HDO (HEALTHCARE DELIVERY ORGANIZATIONS*) di accedere ai dati dei pazienti utilizzando un'applicazione basata sul Web.*

La piattaforma ha implementato criteri di controllo univoci per il controllo degli accessi, l'autenticazione e l'autorizzazione.

1.5 SCENARI

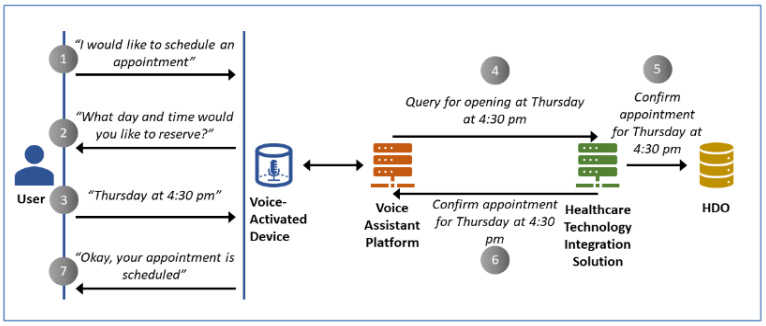
Gli scenari, qui rappresentati, hanno lo scopo di evidenziare il protocollo di colloquio che compone la relazione Paziente-HDO. All'interno della procedura di colloquio, si vedono chiaramente quei sistemi che sono "delicati" per la sicurezza sia dei dati personali sia dell'intero contesto ed in quanto delicati devono essere oggetto di particolare attenzione.

La figure riportate mostrano le interazioni ipotetiche che consentono ai pazienti di interagire con il dispositivo smart home per soddisfare le esigenze della persona.

SCENARIO 1: PROGRAMMAZIONE DELLA VISITA DEL PAZIENTE

1) *Il dispositivo Smart Home può avere funzionalità codificate che riconoscono il comando vocale e attivano la logica dell'applicazione affinché il paziente possa programmare la visita.* (**BIOMETRIA**)
2) *Il sistema fornisce il feedback al paziente consigliando le date e gli orari disponibili per una visita nei sistemi HDO.*

Figure 2-1 Patient Visitation Scheduling



I pallini grigi nella figura, indicano il protocollo di colloquio

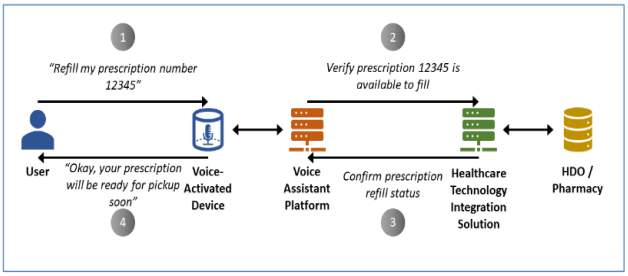
3) *Dopo che il paziente ha selezionato la prenotazione con comandi verbali, la logica applicativa si interfaccia con un sistema di schedulazione.*

➢ **Le interazioni avverranno su Internet pubblico.**

SCENARIO 2: NUOVA PRESCRIZIONE MEDICA PER IL PAZIENTE

1) *Il dispositivo Smart Home applica funzionalità codificate per ricevere il comando vocale e attiva la logica dell'applicazione che stabilisce una sessione di rete con un sistema di informazione del paziente.* (**BIOMETRIA**)
2) *Il sistema informativo del paziente identificherà le prescrizioni del paziente.*

Figure 2-2 Patient Prescription Refill



3) *Il paziente identificherà la prescrizione che vorrebbe avere nuovamente.*
4) *Il sistema di informazione del paziente avrà un'interfaccia per consentire al medico di approvare o rifiutare una richiesta.*
5) *La conferma include lo stato di approvazione o rifiuto e i farmaci sono inoltrati al paziente.*

➢ *Il potenziale flusso di dati considera che i comandi vocali possano offrire un'interfaccia utente a un'applicazione ospitata da una piattaforma di terze parti.*

➢ *L'applicazione può interagire con i sistemi della farmacia per determinare se una prescrizione può essere reinserita fornendo un feedback al paziente come audio sul dispositivo.*

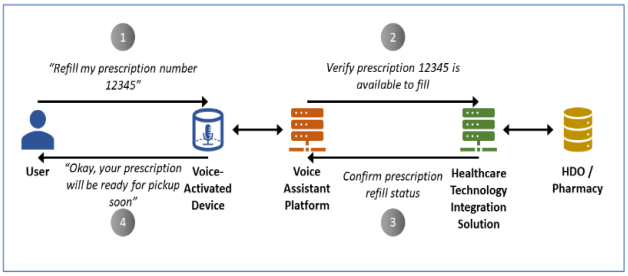
SCENARIO 3: CHECK-IN DEL PAZIENTE

➢ *Il check-in del paziente presuppone che esso possa avere una prescrizione che richieda un'azione regolare e un feedback fornito dal paziente. Un esempio della prescrizione potrebbe essere il monitoraggio dei livelli di dolore.*

➢ **Le interazioni avverranno su Internet pubblico**

1) *Un paziente vocalizza che risponde alla richiesta prescritta.* (**BIOMETRIA**)
2) *Il dispositivo smart home applica funzionalità codificate per ricevere il comando vocale e attiva la logica della applicazione che stabilisce una sessione con un sistema di informazione del paziente.*
3) *Il sistema di informazione del paziente consente a un medico di fornire, ad esempio, un questionario.*

Figure 2-2 Patient Prescription Refill



4) *Il sistema informativo del paziente accede al questionario. L'interrogazione sarà programmatica con domande fornite al paziente via audio.* (**RILEVAZIONE DATI PERSONALI – GDPR**)
5) *Le risposte del paziente sono registrate dal sistema clinico gestito da HDO al fine di gestire il regime del paziente.*

- *La prescrizione può includere la risposta a domande che misurano i livelli di dolore percepito dal paziente su base giornaliera.*
- *I pazienti possono iniziare il regime quotidiano utilizzando i comandi vocali sul proprio dispositivo smart home.*
- *I pazienti possono rispondere alle domande utilizzando l'interazione vocale.*

2. MINACCE

2.1 MINACCE - CASA DEL PAZIENTE

Il dominio domestico del paziente pone diverse sfide quando si considerano le minacce. Nella tabella C-10 sono indicate i rischi relativi all'uso delle funzioni biometriche dei dispositivi domestici.

Esempi:

- *i pazienti o gli operatori sanitari potrebbero non disporre delle risorse o del background tecnologico per affrontare queste minacce in modo indipendente;*
- *i fornitori di piattaforme di telemedicina e gli HDO potrebbero non essere in grado di gestire completamente l'ambiente domestico del paziente;*
- *i pazienti possono avere dispositivi non correlati all'RPM che operano nel loro ambiente domestico;*
- *altre persone all'interno della casa del paziente possono avere accesso fisico ai dispositivi RPM;*

Di seguito si mostrano alcune tabelle aventi lo scopo di indicare le azioni sfavorevoli che possono agire sulle singole componenti o parti di esse.

Nella Tabella C-9 sono indicati i componenti che possono essere presenti nell'ambiente del sistema RPM.

Particolare attenzione deve essere riposta ai BIOMETRIC DEVICE *composti da sensori per la rilevazione degli stati clinici del paziente.* L'USO DI SENSORI NELL'AMBIENTE DOMESTICO RIENTRA NEL SISTEMA IOT.

(La tabella C-9 completa è nel cap. C-7.1 del NIST SP 1800-30)

Table C-9 Components in the Patient Home Environment

Component	Description	Communicates with	Provisioned by
biometric device	A sensor device that interfaces with the patient and captures biometric data that is conveyed to the clinician	patient (direct, tactile interface) interface device wireless personal area network (PAN) (Bluetooth, Wi-Fi) telehealth platform provider (Wi-Fi)	telehealth platform HDO
interface device	A device that potentially retrieves data from biometric devices and is used as a communications device by which patient-clinician communications may occur. The device may be a mobile device such as a tablet or a connected phone running a dedicated application, may be a full-feature device such as a laptop or desktop workstation, or may be a purpose-designed device.	biometric device (e.g., near-field communication[NFC], Bluetooth, Wi-Fi) telehealth platform provider	telehealth platform provider HDO
Wi-Fi access point	A device that provides the RPM environment a wireless means to communicate with devices by using internet protocols	biometric device interface device unrelated equipment	telehealth platform provider HDO patient

La tabella C-10 tratta le azioni sfavorevoli relative ai componenti delle periferiche biometriche.

(La tabella C-10 completa è nel cap. C-7.1 del NIST SP 1800-30)

Table C-10 Biometric Device Subcomponent Breakdown

Subcomponent	Adverse Action	Proximity	C, I, A	Adverse Outcome	Unmitigated Likelihood
tactile interface	An individual other than the patient attaches the biometric device and introduces nonpatient data.	local	I	biometric data would be false; does not pertain to the patient.	high
display	An individual other than the patient may be able to navigate the user interface and view patient biometric data.	local	C	unauthorized individuals may have access to biometric data.	high
display	The display may be damaged so that navigation is not possible.	local	A	biometric device usage degraded	high
onboard storage	Storage media that maintains biometric device system files may be damaged or made unavailable.	local	A	biometric device rendered inoperative	low

La tabella C-11 tratta le azioni sfavorevoli relative alle interfacce dei componenti delle periferiche.

(La tabella C-11 completa è nel cap. C-7.1 del NIST SP 1800-30)

Table C-11 Interface Device Subcomponent Breakdown

Subcomponent	Adverse Action	Proximity	C, I, A	Adverse Outcome	Unmitigated Likelihood
display	Display may become damaged.	local	A	device may be inoperable or unusable.	high
display	An unauthorized individual who has access to the display may be able to obtain biometric	local	A	biometric data lost	low

La tabella C-12 tratta le azioni sfavorevoli relative alle interruzioni dei componenti del laptop.

(La tabella C-12 completa è nel cap. C-7.1 del NIST SP 1800-30)

Table C-12 Laptop Subcomponent Breakdown

Subcomponent	Adverse Action	Proximity	C, I, A	Adverse Outcome	Unmitigated Likelihood
data access port	An individual may access the mobile device and expose	local	I, A	unauthorized code may be introduced that	low

La tabella C-13 tratta le azioni sfavorevoli relative alle interruzioni dei componenti del desktop.

(La tabella C-13 completa è nel cap. C-7.1 del NIST SP 1800-30)

Table C-13 Desktop Subcomponent Breakdown

Subcomponent	Adverse Action	Proximity	C, I, A	Adverse Outcome	Unmitigated Likelihood
data access port	An unintended device may obtain communications channels by using data access ports (e.g., USB).	local	I, A	unauthorized code may be conveyed via the data access port and expose or corrupt subsystem libraries (e.g., operating system).	low
display port	The display port may become	local	A	information may not be displayed; interaction with	low

2.2 MINACCE - TELEHEALTH PLATFORM PROVIDER

Il presupposto è che i fornitori di piattaforme di telemedicina possano implementare controlli pervasivi e disporre di risorse per la privacy e la sicurezza informatica che riducano la probabilità. (VEDI REG. (UE) 2019/881 CYBERSECURITY ACT).

L'avvertenza in queste ipotesi è che le HDO, *che interagiscono con i fornitori di piattaforme di telemedicina, abbiano* **la garanzia che le terze parti coinvolte implementino programmi maturi di privacy e sicurezza informatica**.

Table C-4 Threats Applied to the Telehealth Platform Provider

C, I, A	Threat Event	Description	Likelihood
C	phishing	Telehealth platform provider workforce with privileged access may be susceptible to spear phishing attacks.	high
I, A	malicious software	Telehealth platform provider workforce with privileged access to permitting allows malicious software to be introduced into the telehealth platform environment.	moderate
I, A	command and control	Telehealth platform provider workforce with privileged access to permitting allows threat actors to execute arbitrary code and perform privileged functions.	low
A	ransomware	Ransomware may be introduced into the telehealth platform provider environment either as links or attachments found in phishing emails or may be introduced through local media.	moderate
C	credential escalation	Malware may be introduced to the telehealth platform provider environment that allows threat actors to execute arbitrary code and perform privileged functions.	moderate
I, A	OS or application disruption	Malware may be introduced into the telehealth platform provider environment that disrupts the operating system or applications. Libraries or subsystems may be affected.	low
C	data exfiltration	Sensitive data may be exposed to unauthorized individuals, e.g., via social engineering disclosure or malware that allows threat actors to retrieve data arbitrarily.	moderate

Le origini delle minacce descrivono quei gruppi o individui che possono esporre punti deboli all'infrastruttura RPM (REMOTE PATIENT MONITORING).

Le fonti di minaccia possono intraprendere azioni che espongono o sfruttano le vulnerabilità tramite azioni non intenzionali o attaccando attivamente i componenti all'interno dell'infrastruttura RPM.

La tabella accanto elenca le fonti di minaccia identificate per questa valutazione del rischio.

(La tabella C-6 completa è nel cap. C-5 del NIST SP 1800-30)

Table C-6 Taxonomy of Threat Sources

Type of Threat Source	Description	Characteristics
unintentional–patient	The patient has physical access to biometric devices, workstations, and mobile devices that may be used as part of the RPM patient home environment.	▪ able to access components in patient home domain ▪ intend to access components ▪ patient may be targeted by malicious actors.
unintentional–care provider (e.g., family member, friend, or others with relationship to the patient)	Care providers or other trusted individuals that may have physical access to biometric devices, workstations, and mobile devices that may be used as part of the RPM patient home environment	▪ able to access components in patient home domain ▪ intend to access components ▪ individuals may be targeted by malicious actors.
unintentional–other actors	Other actors may include clinical or technical staff who may be involved in deploying the RPM infrastructure in the patient's home and may have local or remote access to data or systems used as part of the overall RPM system. Other actors may interact with	▪ able to access components or data as part of the RPM system ▪ intend to access the system (e.g., through maintenance or data review) ▪ individuals may be targeted by malicious actors or may represent insider threats

3. VULNERABILITÀ

Di seguito si propone la tabella che identifica le Vulnerabilità con l'indicazione del livello di severità per ognuna di esse.

Table C-8 Vulnerability Taxonomy

Vulnerability Description	Vulnerability Severity	Predisposing Condition	Pervasiveness of Predisposing Condition
Out of Date software	High	*Systems may not have patches deployed in a timely fashion, or software may not be validated to assure that applications may operate appropriately should the underlying operation system receive new updates.*	High
Permissive configuration settings	High	*Underlying operating systems or security components (e.g., firewall) may have configuration settings that allow actions that exceed the minimum necessary to operate the application.*	High
Unmanaged or improperly managed credentials	High	*Applications may use service or other privileged accounts to operate, or operating systems may have privileged accounts that have expansive access to the host system(s). These access privileges may exceed the minimum necessary to operate applications.*	High
Unprotected data	High	*Data on systems may lack restrictions that limit accessibility*	High
Failing or missing integrity or authenticity verification	High	*Data path may lack end-to-end data integrity or authenticity verification.*	High

4. AZIONI SFAVOREVOLI

Nei capitoli precedenti si è parlato di azioni che possono determinare spiacevoli eventi dannosi. Di seguito si propone la tassonomia di tali azioni ed una breve descrizione delle designazioni.

Table 3-2 Problematic Data Action Taxonomy

P, M, D	Problematic Data Action	Description
P, M	Distortion	Inaccurate or misleadingly incomplete data are used or disseminated. Distortion can present users in an inaccurate, unflattering, or disparaging manner, opening the door for stigmatization, discrimination, or loss of liberty. RPM context: Incorrect or unintended use of biometric devices may introduce data quality issues into the RPM environment, resulting in inaccurate or incomplete data being used to make decisions regarding patient care
M	Insecurity	Lapses in data security can result in various problems, including loss of trust, exposure to economic loss and other identity theft-related harms, and dignity losses. RPM context: Biometric data and patient health information flows through various entities in the RPM solution, each of which plays a role in protecting the information.
D, M	Reidentication	De-identified data, or data otherwise disassociated from specific individuals, becomes identifiable or associated with specific individuals again. It can lead to problems such as discrimination, loss of trust, or dignity losses. RPM context: Disassociated processing is intentionally used during some dataflows within the RPM solution to mitigate the risk of exposing identifiable patient information to vendors, administrators, and other practitioners that are outside of the patient's care team.
P, M	Unanticipated revelation	Data reveals or exposes an individual or facets of an individual in unexpected ways. Unanticipated revelation can arise from aggregation and analysis of large and/or diverse data sets. Unanticipated revelation can give rise to dignity losses, discrimination, and loss of trust and autonomy. RPM context: Using one or more biometric devices can indicate potential health problems for which a patient is being monitored to others beyond the patient's healthcare provide.

Questa tassonomia dell'azione problematica sui dati per l'intero sistema RPM *utilizza una designazione di:*

- PREVEDIBILITÀ (**P** - PREDICTABILITY): *consentire ipotesi affidabili da parte di individui, proprietari e operatori sui dati e sulla loro elaborazione da parte di un sistema, prodotto o servizio*
- GESTIBILITÀ (**M** - MANAGEABILITY): *fornire la capacità di amministrazione granulare dei dati, inclusa l'alterazione, la cancellazione e la divulgazione selettiva*
- DISASSOCIABILITÀ (**D** - DISASSOCIABILITY): *consentire il trattamento di dati o eventi senza associazione a persone o dispositivi al di fuori delle esigenze funzionali del sistema*

5. RISCHI

La tabella 3-4 cattura i rischi chiave, assegnando il rischio dove può avere un impatto sugli individui, nelle aree di:

- PREVEDIBILITÀ (**P**REDICTABILITY),
- GESTIBILITÀ (**M**ANAGEABILITY);
- DISSOCIABILITÀ (**D**ISASSOCIABILITY).

I livelli di rischio per la privacy dipendono dal contesto della specifica implementazione della soluzione RPM.

Le tabelle riportate di seguito descrivono la tassonomia nei contesti Cybersecurity e Privacy, rispettivamente la tabella 3-3 e 3-4. Permettendo a chi è incaricato del Risk Management *di avere un quadro abbastanza completo ed una indicazione del metodo di approccio.*

Allo scopo di affrontare con metodo ingegneristico la gestione dei rischi per la privacy, si suggerisce:

1°. *per un approccio iniziale il* "NIST 8062 – AN INTRODUCTION TO PRIVACY ENGINEERING AND RISK MANAGEMENT IN FEDERAL SYSTEMS";

2°. *per l'identificazione dettagliata delle funzioni associate alle categorie dei processi, il* "NIST - PRIVACY FRAMEWORK: A TOOL FOR IMPROVING PRIVACY THROUGH ENTERPRISE RISK MANAGEMENT";

3°. *per l'impostazione delle policy e dei controlli verso i Cloud Provider il* "NIST - PRIVACY FRAMEWORK: A TOOL FOR IMPROVING PRIVACY THROUGH ENTERPRISE RISK MANAGEMENT";

4°. *per la gestione pratica (questionari, ecc.) la metodologia* PRAM (PRIVACY RISK ASSESSMENT METHODOLOGY) del NIST.

Table 3-3 Cybersecurity Risk Taxonomy

C, I, A	RISK	DESCRIPTION	RISK LEVEL
C	Fraudulent use of health-related information	Health-related information may be used for several different fraudulent means, such as identity theft, insurance fraud, or extortion.	Medium
I	Patient diagnoses disrupted based on timeliness disruption, leading to patient safety concerns	Unavailability or significant delay in delivering biometric data may negate the benefits of remote patient monitoring. Clinicians may not be able to provide appropriate care should biometric data transmission be disrupted.	Medium
I	Incorrect patient diagnosis due to change of data	A critical patient event is missed due to changes in the data stream between device and HDO.	High
A	Process disruption due to ransomware	Ransomware may prevent normal device operations. Data may be irretrievable and therefore, may prevent clinical care.	High
I, A	Systemic disruption due to component compromise	Disruptions to the system that affect its availability or integrity may compromise the benefits derived from remote patient monitoring.	High
I	Clinician misdiagnosis	If data are altered inappropriately, clinicians may make inaccurate diagnoses, resulting in patient safety issues.	High

Table 3-4 Privacy Risk Taxonomy

P, M, D	Risk	Problematic Data Action
M	Unauthorized individuals may access data on devices	Insecurity: Data not protected at rest or in transit
P, M	Biometric device types can indicate patient health problems that individuals would prefer not to disclose beyond their healthcare provider	Unanticipated revelation: Biometric device types can indicate patient health problems individuals would prefer not to disclose beyond their healthcare provider.
P, M	Incorrect data capture of readings by devices may impact quality of patient care	Distortion: Device misuse may cause failure to monitor patients in accordance with their healthcare plan.

D, M	Aggregated data may expose patient information	Re-identification: Associating biometric data with patient identifiers can expose health conditions.
P, M	Exposure of patient information through multiple providers of system components	Unanticipated Revelation: Data sharing across parties can increase the risk of exposure due to confidentiality-related incidents, which can reveal patient health information in ways or to parties that the individual may not expect.

6. ZERO TRUST

L'architettura della Telemedicina può essere ricondotta nel paradigma di Zero Trust.

L'Appendice F del NIST SP 1800-30B Applicazione del modello OSI per comprendere l'architettura Zero Trust

L'ISO e l'IEC descrivono il modello OSI come composto da sette livelli denominati:

7° *livello:* APPLICAZIONE,

6° *livello:* PRESENTAZIONE,

5° *livello:* SESSIONE,

4° *livello:* TRASPORTO,

3° *livello:* RETE,

2° *livello:* COLLEGAMENTO DATI,

1° *livello:* FISICO,

in cui i livelli sono numericamente ordinati al contrario.

Cioè, il livello di applicazione è considerato come **Livello 7**, *mentre il livello fisico è considerato come livello 1, una prova di concetto per proteggere le sessioni di rete tra la casa del paziente e il fornitore della piattaforma di telemedicina.*

I dispositivi che operano al **Livello 2** *hanno indirizzi* MAC (MEDIA ACCESS CONTROL) *mediante i quali i dispositivi, come i dispositivi biometrici, possono comunicare attraverso un segmento di rete locale (LAN).*

Le soluzioni **Livello 2** *e* **Livello 3** *consentono ai dispositivi che non implementano il livello di rete di avere un'interconnettività più ampia. E forniscono sicurezza limitando l'accesso ai dispositivi e proteggendo le comunicazioni in transito dei dati, ad esempio con la crittografia.*

Le organizzazioni possono prendere in considerazione soluzioni Layer 2 su Layer 3 per dispositivi che potrebbero essere soggetti a minacce Internet.

I dispositivi biometrici possono implementare l'interconnettività **Livello 2** *e* **Livello 3**; *tuttavia, non dispongono di controlli robusti che impediscono l'accesso remoto non autorizzato.*

La pubblicazione "NIST (SP) 800-207 ZERO TRUST ARCHITECTURE" *descrive un modello di* GATEWAY ENCLAVE *che può essere applicato a un'architettura di telemedicina per il monitoraggio remoto del paziente (*Telehealth REMOTE PATIENT MONITORING – RPM - Architecture*).*

Nel modello del gateway dell'enclave, una soluzione ZERO TRUST *opera su due piani concettuali:*

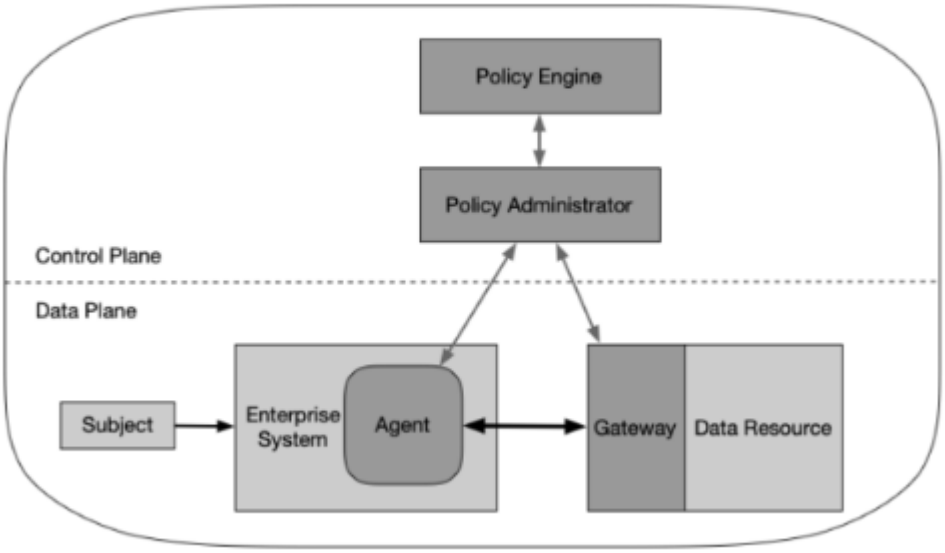
1. PIANO *di* CONTROLLO (CONTROL PLANE)
2. PIANO DATI (DATA PLANE).

I dispositivi di gestione della microsegmentazione operano in un PIANO DI CONTROLLO (CONTROL PLANE). *Questi dispositivi di gestione forniscono funzionalità amministrative e di policy per supportare enclave sicure.*

I componenti operativi, come dispositivi biometrici, servizi di provider di piattaforme di telemedicina e dispositivi ospitati da organizzazioni di assistenza sanitaria, possono operare nel PIANO DATI (DATA PLANE).

La Figura F-1 mostra il modello di gateway dell'enclave.

Figure F-1 Enclave Gateway Model [25]



La soluzione **Livello** *2 e* **Livello** *3 utilizzata in questa guida pratica introduce i principi sull'architettura* ZERO TRUST (ZTA) all'RPM *di telemedicina.*

I dispositivi biometrici gestiti possono essere soggetti a minacce che possono essere presenti nella rete domestica del paziente.

L'approccio **Livello** *2 e* **Livello** *3 segmenta i componenti* RPM *di altri dispositivi che possono operare nella casa del paziente.*

I dispositivi non associati ai componenti RPM *distribuiti non dispongono di un percorso di comunicazione con i dispositivi* RPM.

> *ZTA consente ai dispositivi biometrici di autenticarsi nella soluzione di sicurezza* **Livello 2** *e* **Livello** 3 *in modo che solo il traffico proveniente dai componenti RPM attraversi la rete* **Livello** 2 *e* **Livello** 3.

Chi è interessato può fare riferimento al "NIST SP 800-207 ZERO TRUST ARCHITECTURE".

7. RIFERIMENTI

1) NIST IR 8334 - Using Mobile Device Biometrics for Authenticating First Responders
2) NIST IR 8062 – An Introduction to Privacy Engineering and Risk Management in Federal Systems
3) NIST - Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management
4) NIST SP 1800-30 – Securing Telehealth Remote Patient Monitoring Ecosystem
5) NIST – Mitigating Cybersecurity Risk in Telehealth Smart Home Integration
6) NIST – Privacy Enhanced Identity Brokers