Analisi dei Rischi - PatientMonitoring

Jacopo Levati

7 luglio 2025

Descrizione del progetto

PatientMonitoring è un'ipotetica applicazione mobile per il monitoraggio dei parametri vitali di pazienti cronici. Sono previsti due tipologie di utenti: pazienti e medici. L'applicazione ha l'obiettivo di raccogliere i parametri vitali dei pazienti, come: ECG, pressione sanguigna, glicemia, il respiro, posizione e spostamenti e di trasmetterli ai rispettivi medici che li hanno in cura. La misurazione dei parametri vitali avviene attraverso l'impiego di dispositivi indossabili come smartwatch e cardiofrequenzimetro a fascia toracica. L'idea dell'applicazione è, inoltre, di monitorare costantemente la posizione dei pazienti, rendendo possibile, in caso di emergenza, eventuali interventi nell'immediato. L'applicazione, in caso di valori di parametri fuori norma, invia notifiche, suggerendo al paziente possibili rimedi, prescritti dal medico, per ripristinare i parametri. Consente, invece, ai medici di accedere e monitorare la situazione dei propri pazienti, con la possibilità di contattarli in caso di urgenza o per programmare visite di controllo.

Descrizione delle Funzionalità

Funzionalità dell'app

- **Login**: sono previste due tipologie di utenti, ovvero pazienti e medici.
- **Monitoraggio dei parametri**: i dati raccolti sono visibili in tempo reale sia dai pazienti che dai medici che li hanno in cura.
- **Contatto diretto con medici**: i pazienti potranno contattare direttamente i propri medici attraverso messaggi o chiamate.
- **Prenotazioni visite**: entrambi gli utenti possono richiedere e fissare una visita di controllo.
- **Notifiche**: in caso di parametri fuori norma, sia il paziente che il medico vengono immediatamente avvisati.

- **Posizione in tempo reale**: permette al medico curante di avere sempre monitorata la posizione dei propri pazienti.
- **Storico e andamento dei parametri**: i pazienti e i medici possono accedere a grafici e statistiche sull'andamento dei parametri vitali nel tempo, utili per valutare l'evoluzione dello stato di salute e l'efficacia delle terapie.
- **Gestione del piano terapeutico**: il medico può inserire o aggiornare il piano terapeutico.
- **Riepilogo automatico delle visite**: dopo ogni visita viene generato automaticamente un report consultabile con sintesi dei parametri, diagnosi e azioni intraprese.

Identificazione dei Rischi

Part-A - Product Engineering

Sl.No.	Attributo	Descrizione	Valutazione Sì/No	Può causare un rischio?
PE1 Requisiti				
PE1.a	Stabilità	I requisiti cambiano anche durante la produzione del prodotto?	No	No
PE1.b	Completezza	I requisiti mancano o sono specificati in modo incompleto?	No	No
PE1.c	Chiarezza	I requisiti non sono chiari o necessitano di interpretazione?	No	No
PE1.d	Validità	I requisiti portano al prodotto che il cliente ha in mente?	Sì	No
PE1.e	Fattibilità	I requisiti non sono realizzabili da un punto di vista analitico?	No	No

PE1.f	Precedente	I requisiti specificano qualcosa che è nuovo o che <azienda> non ha mai fatto prima?	Sì	Sì
PE1.g	Scala	I requisiti specificano quanto segue: • Il prodotto è grande, più complesso oppure • Richiede un'organizzazione più grande dell'esperienza aziendale esistente?	No	No
PE2. Design				
PE2.a	Funzionalità	Ci sono potenziali problemi nel soddisfare i requisiti di funzionalità?	Sì	Sì. Il progetto ha molte funzionalità complesse (monitoraggio parametri, notifiche in tempo reale, contatto medico, geolocalizzazione) e soddisfarle tutte in modo fluido e completo può rappresentare un rischio di progettazione.
PE2.b	Difficoltà	La progettazione e/o l'implementazione sono difficili da realizzare?	Sì	Sì. La progettazione è complessa, soprattutto per quanto riguarda l'integrazione di dispositivi wearable, l'affidabilità del rilevamento e il rispetto delle normative in ambito sanitario.
PE2.c	Interfacce	Le interfacce interne (hardware e software) sono ben definite e controllate?	No	Sì

PE2.d	Performance	• I criteri di prestazione sono chiaramente indicati e sono realizzabili? • Sono previsti tempi di risposta o velocità effettiva rigorosi	No	No.
PE2.e	Testabilità	Il prodotto è difficile o impossibile da testare?	No	No. Il prodotto è testabile, anche se richiede l'uso di dispositivi esterni (wearable).
PE2.f	Vincoli hardware	C'è un vincolo stretto sull'hardware di destinazione?	Sì	Sì. Anche se l'app gira su dispositivi mobili comuni, dipende fortemente da dispositivi wearable compatibili, che potrebbero avere limiti di hardware (sensori non supportati)
PE2.g	Software non di sviluppo	Il riutilizzo o l'acquisto di software da utilizzare nel progetto porta a problemi quali: • Prestazione • Mancanza di documentazione, ecc.	No	No. In caso l'app utilizzi SDK ufficiali. Se si decide di integrare librerie di terze parti poco documentate, il rischio potrebbe aumentare.
PE3. Codice e test unitari				
PE3.a	Fattibilità	L'implementazione del design è difficile o impossibile?	No	No

PE3.b	Testing	Il livello e il tempo specificati per i test unitari sono adeguati?	/	Sì. Alcune funzionalità (integrazione con l'hardware, geolocalizzazione e invio di notifiche) possono risultare difficili da testare in isolamento. Potrebbero richiedere dei test di integrazione o simulazioni.
PE3.c	Codifica / Implementazione	Ci sono problemi con la codifica e l'implementazione, ad esempio: • Disponibilità di progettazione dettagliata • Vincoli di sistema come temporizzazione, memoria esterna, memoria ecc.	No	No
PE4. Integrazione e test				
PE4.a	Ambiente	L'ambiente di integrazione e di test è adeguato?	/	No. Se l'ambiente prevede simulazione dei wearable, testing mobile su più dispositivi e ambiente di backend.
PE4.b	Prodotto	I seguenti fattori sono adeguati? • Definizioni delle interfacce • Attrezzatura • Ore	/	Sì. La disponibilità di alcuni dispositivi wearable potrebbe essere incerta e le interfacce sono ancora in fase di definizione.

PE4.c	Sistema	a) Esiste un coordinamento dell'integrazione di sistema? b) I seguenti fattori sono adeguati: • Definizione dell'interfaccia • Attrezzatura	No	Sì. Il progetto è ancora in una fase di progettazione. Le interfacce non sono ancora state definite in modo chiaro e il sistema di coordinamento non è stato ancora deciso.
PE5. Specialità ingegneristiche				
PE5.a	Manutenibilità	L'implementazione è difficile da capire o da mantenere?	No	No. Il codice verrà strutturato in modo modulare e si useranno tecnologie comuni.
PE5.b	Affidabilità	I requisiti di affidabilità o disponibilità sono difficili da soddisfare?	Sì	Sì. Il sistema deve funzionare 24/7, notificare emergenze, sincronizzare dati vitali. Tutti requisiti ad alta affidabilità, difficili da garantire costantemente in condizioni reali (rete, batteria, ...).
PE5.c	Sicurezza	I requisiti di sicurezza sono fattibili e dimostrabili?	No	Sì. Non esiste ancora un piano per protezione dati e crittografia.
PE5.d	Sicurezza	I requisiti di sicurezza sono più rigorosi rispetto allo stato attuale della pratica o dell'esperienza del programma?	Sì	Sì. Trattando dati sanitari, i requisiti di sicurezza devono seguire normative stringenti.
PE5.e	Fattori umani	Il sistema è difficile da usare a causa della scarsa definizione dell'interfaccia umana?	No	No. L'app è progettata con UI/UX moderne.

PE5.f	Specifiche	La documentazione è adeguata per: • Design • Implementazione • Testare il sistema	No	Sì. La documentazione è critica per design, sviluppo, testing e validazione in ambito medico.

Parte B - Ambiente di sviluppo

DE1. Processo di sviluppo				
DE1.a	Idoneità	Il modello di processo è adatto a soddisfare i requisiti del progetto?	Sì	No. Se si segue un modello strutturato (Agile, Scrum, ...). Serve comunque una gestione iterativa, vista la complessità.
DE1.b	Controllo di processo	I siti di sviluppo distribuiti sono coordinati?	No	Sì. Esistono collaborazioni esterne (servizi cloud e fornitori di dispositivi).
DE1.c	Dimestichezza	Tutti i membri del personale sono a conoscenza del processo da seguire?	/	/
DE1.d	Controllo del prodotto	Esistono meccanismi per controllare le modifiche nel prodotto?	No	Sì. La mancanza di controllo delle modifiche è un rischio serio e non è ancora stato implementato. Bisognerebbe utilizzare strumenti come Git, un sistema di gestione dei cambiamenti e procedure di revisione.
DE2. Sistema di sviluppo				

DE2.a	Capacità	Le seguenti condizioni sono sufficienti: • Workstation • Potenza di elaborazione • Memoria • Capacità di archiviazione	/	/
DE2.b	Idoneità	Il sistema di sviluppo supporta tutte le fasi, le attività e le funzioni?	/	/
DE2.c	Usabilità	Il sistema di sviluppo è facile da usare?	/	/
DE2.d	Dimestichezza	Il team di progetto conosce il sistema di sviluppo e il cliente?	/	/
DE2.e	Affidabilità	Il sistema soffre di bug del software, tempi di inattività e backup integrato insufficiente?	/	Sì
DE2.f	Supporto di sistema	Esiste un supporto tempestivo da parte di esperti o fornitori per il sistema?	Sì	Sì. Trattandosi di dati medici è avere supporto e intervento tempestivo è fondamentale.
DE2.g	Recapito	Sono stati definiti i requisiti di definizione e accettazione per la consegna del sistema di sviluppo al cliente?	No	No.
DE3. Processo di gestione				

DE3.a	Pianificazione	• La pianificazione è tempestiva? • Il piano include approccio tecnico e piano di emergenza? • Tutti gli elementi della WBS sono stati rivisti?	No	Sì
DE3.b	Progetto Organizzazione	I ruoli e le relazioni di reporting sono chiari?	/	/
DE3.c	Esperienza di gestione	I manager sono esperti in: • Sviluppo software • Gestione del software • Il dominio dell'applicazione • Il processo di sviluppo • Su programmi di grandi dimensioni	/	Sì. Vista la natura del progetto, è fondamentale che i manager abbiano esperienza.
DE3.d	Interfacce del programma	C'è una scarsa interfaccia con il cliente, altri appaltatori, senior e/o peer manager?	/	/
DE4. Metodi di gestione				
DE4.a	Gestione della configurazione	Le procedure di controllo delle modifiche o il controllo delle versioni, inclusi i siti di installazione, sono adeguati?	/	Sì
DE5. Ambiente di lavoro				

DE5.a	Comunicazione	C'è scarsa consapevolezza della missione o degli obiettivi, scarsa comunicazione delle informazioni tecniche tra colleghi e manager?	/	Sì

Parte C - Vincoli del programma

PC1. Risorse				
PC1.a	Programma	Il programma è inadeguato o instabile?	/	Sì
PC1.b	Staff	Il personale manca nei seguenti: • Esperienza • Mancanza di conoscenza del dominio • Abilità • Carente	/	No. Nel caso il team non sia nuovo al dominio sanitario.
PC1.c	Hardware/ Software	I ritardi nella valutazione hardware/software e nell'approvvigionamento comportano dei rischi?	No	No
PC1.d	Attrezzatura	Le strutture sono adeguate per la costruzione e la consegna del prodotto?	Sì	No
PC2. Contratto				
PC2.a	Tipo di contratto	Il tipo di contratto è una fonte di rischio per il programma?	/	/

PC2.b	Restrizioni	Il contratto comporta delle restrizioni?	Sì	Sì. Il contratto, essendo in ambito sanitario, dovrà rispettare normative vincolanti sul trattamento dei dati (GDPR, privacy sanitaria), conformità dei dispositivi medici.
PC2.c	Dipendenze	Il programma ha dipendenze da prodotti o servizi esterni?	Sì	Sì. Il sistema dipende da dispositivi wearable esterni e servizi software esterni (notifiche push, geolocalizzazione, API mediche, cloud storage)
PC3. Interfacce di programma				
PC3.a	Cliente	Ci sono problemi con i clienti come: • Lungo ciclo di approvazione dei documenti • Scarsa comunicazione, • Competenza di settore inadeguata?	Sì	Sì. Il cliente è rappresentato da enti sanitari o medici. Questo può comportare ritardi nelle approvazioni. Ciò può rallentare lo sviluppo.
PC3.b	Fornitori	I fornitori rispondono alle esigenze dei programmi?	Sì	Sì. Poiché il progetto dipende da dispositivi wearable e servizi di terze parti, eventuali problemi di disponibilità, compatibilità o supporto fornitori possono costituire un rischio concreto per tempistiche e affidabilità.

Un'applicazione come PatientMonitoring, dedicata al monitoraggio dei parametri vitali di pazienti cronici, comporta rischi significativi sia di prodotto che di processo, data la sua delicatezza e l'impatto potenziale sulla salute delle persone. Di seguito una distinzione e analisi dei principali rischi:

Rischi di Prodotto

- **Affidabilità dei dati**: Siccome l'applicazione è pensata per misurare costantemente i parametri dei pazienti, letture scorrette dei parametri vitali (es. frequenza cardiaca errata, glicemia non aggiornata) possono comportare diagnosi sbagliate, mancati interventi in situazioni critiche, falsi allarmi.
- **Ritardi nella trasmissione dei dati**: i parametri reali non vengono trasmessi in tempo reale. Di conseguenza: medici non aggiornati, rischi per la vita del paziente in situazioni d'emergenza.
- **Malfunzionamenti del sistema di notifiche**: notifiche di allarme non inviate o non ricevute. Potrebbe comportare un mancato intervento tempestivo in caso di necessità.
- **Interfaccia utente poco chiara o complessa**: pazienti, spesso anziani, non capiscono come usare l'app. Dati non consultati, funzionalità non sfruttate, confusione nei momenti di emergenza.
- **Problemi di compatibilità con dispositivi wearable**: l'app non comunica bene con smartwatch, fasce toraciche.

Rischi di Processo

- **Test inadeguati o poco realistici**: test svolti solo in laboratorio, senza scenari reali con pazienti. Di conseguenza: possibile presenza di bug non rilevati, sistema non affidabile, che potrebbe condurre a problemi gravi in quanto l'applicazione tratta dati vitali.
- **Dipendenza da fornitori esterni**: problemi tecnici con i produttori di dispositivi indossabili. Possibile interruzione del servizio, necessità di adattamento costosi.

Rischi di Sicurezza

- **Violazione della privacy dei dati sanitari**: accesso non autorizzato a dati medici (ECG, glicemia, posizione). Violazioni di questo genere potrebbero comportare danni reputazionali, multe, potenziale uso malevolo dei dati.
- **Intercettazione dei dati in transito**: L'app raccoglie e invia vari dati (dati di prenotazione delle visite, contatti, dati di pagamento, dati relativi alla posizione, parametri vitali). Se non viene garantita la conformità a normative sulla privacy, o se il sistema di cifratura e protezione non fosse adeguato, si potrebbe verificare fuga di dati sensibili con conseguenti danni legali.
- **Accessi non autorizzati**: utenti malintenzionati accedono a profili di pazienti o medici usando credenziali rubate o troppo deboli. Conseguenze: lettura o modifica dei dati, con possibili manomissioni pericolose.

- **Autorizzazioni sbagliate nei ruoli utente**: pazienti che vedono dati di altri pazienti, o medici che accedono a cartelle non assegnate. Gravi violazioni della riservatezza.

Prioritizzazione dei Rischi

Rischio	**P(UO)**	**L(UO)**	**RE**	**Note**
Affidabilità dei dati	8	10	80	L'errore nei dati clinici può portare a diagnosi sbagliate o mancate emergenze. Essendo trasmessi da dispositivi esterni e automatizzati, l'affidabilità è critica.
Accessi non autorizzati	8	10	80	Sistema sanitario corrisponde a dati sensibili. La probabilità di attacchi è alta e le conseguenze (furto dati) sono massimi.
Ritardi di trasmissione dati	7	10	70	La comunicazione in tempo reale è un aspetto fondamentale per l'intervento d'emergenza. Rischio molto probabile su reti mobili o dispositivi poco affidabili.
Violazione privacy dati	7	10	70	Il rischio è legato al mancato rispetto del GDPR e alla presenza di dati clinici, posizione GPS, ... alta probabilità (interconnessioni multiple, API, cloud) e impatto elevatissimo (sanzioni e reputazione).
Intercettazione dati in transito	6	10	60	I dati viaggiano via internet, che è un canale vulnerabile. Senza cifratura avanzata (TLS), il rischio è elevato e l'impatto è massimo.
Malfunzionamenti notifiche	7	10	70	Se una notifica (avviso medico o suggerimento urgente) non arriva, il paziente non è consapevole di dover intervenire.

Autorizzazioni errate	5	9	45	Il controllo degli accessi e dei ruoli (medico/paziente) deve essere preciso. Una configurazione errata può esporre dati non autorizzati.
Test non realistici	7	9	63	Se i test non coprono casi reali (pazienti che compiono azioni quotidiane, reti instabili, ...) è possibile che il rischio di errori critici non rilevati aumenti.
Compatibilità dispositivi	7	7	49	L'app dipende da diversi dispositivi. Alcuni potrebbero non essere supportati bene, causando perdita di dati.
Dipendenza fornitori esterni	5	8	40	Se un fornitore cambia politica o interrompe il servizio, il rischio non è trascurabile e impatta economicamente e tecnicamente.
Interfaccia utente poco chiara per anziani	7	6	42	Il target comprende persone anziane o poco digitalizzate. L'usabilità complessa può ridurre l'adozione, ma non ha un impatto vitale.

Gestione dei Rischi e Piano di Contingenza

Affidabilità dei dati

- **Azioni preventive:**
  - Implementare controlli automatici di coerenza e qualità dei dati ricevuti (range validi)
  - Utilizzare algoritmi di validazione incrociata tra diversi parametri (ECG anomale + battito basso)
  - Certificare i dispositivi compatibili e monitorare periodicamente le prestazioni
- **Piano di contingenza:**
  - Bloccare temporaneamente l'invio ai medici di dati considerati non affidabili
  - Inviare un alert al medico

  - Registrare l'anomalia per un miglioramento algoritmico

Accessi non autorizzati

- **Azioni preventive:**
  - Autenticazione a due fattori per i medici
  - Protezione da brute force attacks, timeout automatici e login continuo degli accessi
  - Formazione interna su gestione password
- **Piano di contingenza:**
  - Blocco automatico degli account compromessi
  - Reset forzato delle credenziali
  - Indagine per rilevare altri account a rischio e ripristino dei dati alterati

Ritardi nella trasmissione dei dati

- **Azioni preventive:**
  - Implementare un meccanismo di invio asincrono con retry automatico e salvataggio locale in caso di assenza di rete
  - Ottimizzare la compressione e il peso dei dati trasmessi
- **Piano di contingenza:**
  - Attivare una trasmissione d'emergenza via SMS
  - Informare il medico del ritardo con segnalazione dell'ultimo timestamp disponibile

Violazione della privacy dei dati sanitari

- **Azioni preventive:**
  - Crittografia dei dati in storage e in transito
  - Audit regolari sui sistemi di sicurezza
  - Implementazione di politiche GDPR e consenso esplicito da parte dell'utente
- **Piano di contingenza:**
  - Notificare l'autorità di controllo e gli utenti interessati
  - Bloccare e indagare sull'origine della violazione, con disattivazione temporanea dei moduli compromessi

Intercettazione dei dati in transito

- **Azioni preventive:**
  - Utilizzo esclusivo di HTTPS/TLS + certificati validi
  - Verifica della sicurezza delle reti da cui avviene la trasmissione
  - Nessun dato sensibile in chiaro nei log o nelle richieste
- **Piano di contingenza:**
  - Disattivazione temporanea delle comunicazioni non sicure
  - Rotazione delle chiavi di cifratura

Malfunzionamento delle notifiche

- **Azioni preventive:**
  - Test end-to-end su vari dispositivi e sistemi operativi
  - Utilizzare sistemi di backup alternativi per le notifiche, come SMS e e-mail
- **Piano di contingenza:**
  - Se una notifica non viene ricevuta, attivare automaticamente il canale di backup

Autorizzazioni sbagliate nei ruoli utente

- **Azioni preventive:**
  - Implementazione rigorosa di Role-Based Access Control
  - Test automatici su permessi e visibilità dati
- **Piano di contingenza:**
  - Revoca immediata dei permessi non corretti
  - Notifica agli utenti coinvolti
  - Correzione dei dati accessibili e registrazione dell'incidente

Test inadeguati o non realistici

- **Azioni preventive:**
  - Effettuare test in contesti reali con pazienti e medici veri
  - Introdurre fasi di beta testing con raccolta feedback
- **Piano di contingenza:**
  - Se emergono bug critici non previsti, attivare immediatamente rollback alla versione precedente
  - Comunicare ai medici la limitazione temporanea della funzionalità interessata

Problemi di compatibilità con dispositivi wearable

- **Azioni preventive:**
  - Redigere una lista ufficiale di dispositivi certificati
  - Test di compatibilità
  - Utilizzare protocolli standard (bluetooth LE)
- **Piani di contingenza:**
  - Proporre un dispositivo alternativo certificato

Dipendenza da fornitori esterni

- **Azioni preventive:**
  - Usare API standard per facilitare l'integrazione con più fornitori
  - Tenere aggiornato un sistema di fallback con dispositivi alternativi
- **Piano di contingenza:**
  - Passare a fornitore alternativo (già validato) in caso di disservizio prolungato

Interfaccia utente poco chiara o complessa

- **Azioni preventive:**
  - Coinvolgere pazienti anziani nei test di usabilità
  - Utilizzare caratteri grandi e interazioni minime
  - Includere tutorial vocali per l'uso

  - Aggiungere una modalità semplificata attivabile dal medico

- **Piano di contingenza:**
  - Fornire assistenza remota per supportare l'utente