**Min hälsoplan**

**Riskanalys inkl. rapport och åtgärder**

**Revisionshistorik**

|  |  |  |  |
| --- | --- | --- | --- |
| **Datum** | **Version** | **Beskrivning** | **Författare** |
| 2015-02-25 | PA1 | Första versionen | AF |

**Innehållsförteckning**

1 Inledning 5

2 Syfte 5

3 Metod för riskanalys 5

4 Riskanalys 6

4.1 Steg 1 – Initial analys 6

4.2 Steg 2 – fördjupad analys 7

5 Riskanalysrapport 8

**Definitioner och Referenser**

**Definitioner**

|  |  |
| --- | --- |
| **Term** | **Beskrivning** |
|  |  |
|  |  |

**Referenser**

|  |  |
| --- | --- |
| **Dokument** | **Länk** |
| Min hälsoplan webb | <http://www.minhalsoplan.se> |
| Min hälsoplan programvara | <https://github.com/MinHalsoplan/netcare-healthplan> |
| Min hälsoplan demo | <http://46.137.134.138/v2/netcare> |
| GitFlow | <http://nvie.com/posts/a-successful-git-branching-model> |

# Inledning

Min hälsoplan är en e-hälsotjänst i Mina vårdkontakter där vårdpersonal och patienter tillsammans skapar en hälsoplan. Hälsoplanen innehåller en eller flera aktiviteter som patienten får påminnelse att göra, samt kan han eller hon rapportera in resultat från aktiviteten direkt till personalen. Syftet med Min hälsoplan är att stötta både patient och personal under en kort eller lång uppföljning genom att öka tillgänglighet och kvalitet på information samt skapa en ökad kontinuitet i vårdprocessen.

Se även: <http://www.minhalsoplan.se>

# Syfte

Detta dokument innehåller resultatet av genomförd riskanalys, inklusive rapport och åtgärder.

# Metod för riskanalys

Riskanalysen genomförs i två steg. Steg 1 – initial riskanalys – gör en genomgång av samtliga identifierade risker. För varje risk bedöms allvarlighetsgrad och sannolikhet enligt klassningen i Tabell 1 nedan. En riskpoäng räknas ut genom att multiplicera allvarlighetsgrad med sannolikhet. Om riskpoängen överstiger ett visst tröskelvärde (8) behövs fördjupad analys som sker i steg 2.

I steg 2 sker en förd analys av utvalda risker. I detta ingår analys av varje risks underliggande orsaker samt förslag till åtgärder och uppföljning.

Slutligen sammanställs en riskanalysrapport där riskpoäng beräknas med hänsyn till gjorda åtgärder.

|  |  |  |  |
| --- | --- | --- | --- |
| **Allvarlighetsgrad** | | **Sannolikhet** | |
| 1 | Mycket obetydlig konsekvens | 1 | Mycket låg sannolikhet |
| 2 | Obetydlig konsekvens | 2 | Låg sannolikhet |
| 3 | Konsekvens av medelstor betydelse | 3 | Medelstor sannolikhet |
| 4 | Allvarlig konsekvens | 4 | Hög sannolikhet |
| 5 | Mycket allvarlig konsekvens | 5 | Mycket hög sannolikhet |

Tabell Klassning av allvarlighetsgrad och sannolikhet

# Riskanalys

## Steg 1 – Initial analys

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Risk** | | **Initial riskbedömning** | | | **Kommentar till analys** | **Fördjupad analys?** |
| **Risk-id** | **Beskrivning** | **Allvarlighetsgrad** | **Sannolikhet** | **Riskpoäng** |  |  |
|  | ***Projektrisker*** |  |  |  |  |  |
| RP1 | Kravbilden är otydlig | 4 | 3 | 12 |  | JA |
| RP2 | Otillräcklig nytta för användare | 5 | 1 | 5 | Tätt samarbete med användarrepresentanter gör att sannolikheten bedöms låg. |  |
| RP3 | Kan ej få fram önskad funktionalitet inom avdelad budget. | 3 | 3 | 9 |  | JA |
| RP4 | Brist på engagemang för projektet från användarna | 4 | 2 | 8 | Motiverade användare i referensgruppen gör sannolikheten relativt låg. |  |
| RP5 | Kraven missuppfattas av utvecklingsgruppen | 4 | 3 | 12 |  | JA |
| RP6 | Användning av ny/oprövad teknik | 3 | 2 | 6 | Väl avvägd användning av modern men beprövad teknik gör sannolikheten relativt låg. |  |
| RP7 | Brist på rätt kompetens hos utvecklingsgruppen | 5 | 1 | 5 | Seniora utvecklare med hög kompetens inom relevanta områden gör sannolikheten låg. |  |
|  | ***Kvalitetsrisker*** |  |  |  |  |  |
| RK1 | Dålig stabilitet/upptid | 4 | 3 | 12 |  | JA |
| RK2 | Stor mängd buggar | 3 | 3 | 9 |  | JA |
| RK3 | Otillräcklig prestanda – långa svarstider | 3 | 2 | 6 | Systemets komplexitet och belastning bedöms måttlig, varför sannolikheten är relativt låg. |  |
| RK4 | Felaktigheter i data som hanteras | 5 | 2 | 10 |  | JA |
| RK5 | Data blir korrupt eller förstörs | 5 | 2 | 10 |  | JA |
|  | ***Säkerhetsrisker*** |  |  |  |  |  |
| RS1 | Ej behörig användare kan logga in i systemet | 5 | 3 | 15 |  | JA |
| RS2 | Otillåten åtkomst av data | 5 | 3 | 15 |  | JA |

## Steg 2 – fördjupad analys

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Risk** | |  | **Orsak** | **Åtgärd** | **Uppföljning** |
| **Risk-id** | **Beskrivning** | **Riskpoäng** |  |  |  |
|  | ***Projektrisker*** |  |  |  |  |
| RP1 | Kravbilden är otydlig | 12 | Heltäckande kravspecifikation saknas. | Använd agil utvecklingsmetod (Scrum). Krav prioriteras löpande. Kontinuerlig feedback Sprint-demos. | Löpande uppföljning i samband med Sprint-demo och Sprint-retrospective. |
| RP3 | Kan ej få fram önskad funktionalitet inom avdelad budget. | 9 | För stor kravmassa. Otillräcklig prioritering av krav. | Fokusera på prioriterade krav och att slopa mindre viktiga krav. | Löpande i samband med Sprint-planering. |
| RP5 | Kraven missuppfattas av utvecklingsgruppen | 12 | Otytdligt formulerade krav. För lång feedback-loop. | Tydlig beskrivning av krav i backlogg. Kort Sprint-längd (2 v). Löpande kontakt mellan Scrum-master och Produktägare under Sprinten. | Löpande uppföljning i samband med Sprint-demo och Sprint-retrospective. |
|  | ***Kvalitetsrisker*** |  |  |  |  |
| RK1 | Dålig stabilitet/upptid | 12 | Brister i arkitektur (för komplex, ej adekvat för ändamålet)  Ej ändamålsenlig driftsmiljö. | Skapa en robust grundarkitektur tidigt i projektet.  Kravställ och följ upp driftsaspekter redan från projektstart. | Löpande uppföljning i samband med Sprint-demo och Sprint-retrospective. |
| RK2 | Stor mängd buggar | 9 | Otillräcklig testning. | Automatiserade unit-tester används i så stor omfattning som möjligt. Användargruppen funktionstestar kontinuerligt. | Löpande uppföljning i samband med Sprint-demo och Sprint-retrospective. |
| RK4 | Felaktigheter i data som hanteras | 10 | Otillräcklig validering. Otydliga instruktioner/ledtexter. | Säkerställ validering av all inmatning. Enkla och tydliga instruktioner/ledtexter. | Löpande uppföljning i samband med Sprint-demo och Sprint-retrospective. |
| RK5 | Data blir korrupt eller förstörs. | 10 | Systemfel eller hårdvarufel. | Tillse att tydliga driftsinstruktioner tas fram. | Följ upp tillämpning av driftsinstruktioner med driftsleverantör. |
|  | ***Säkerhetsrisker*** |  |  |  |  |
| RS1 | Ej behörig användare kan logga in i systemet | 15 | Osäkra mekanismer för autentisering. | Använd vedertagna metoder för säker autentisering (Bank ID, MVK) | Följ upp efterlevnad av säkerhetslösning. |
| RS2 | Otillåten åtkomst av data | 15 | Obehörig kan utnyttja säkerhetsluckor för att komma åt data. | Genomför penetrationstest och vidta korrigerande åtgärder. | Granskning av resultat från penetrationstest, uppföljning av åtgärder. |

# Riskanalysrapport

Nedan ges en sammanställning av samtliga identifierade risker. För varje risk anges initial riskbedömning, om åtgärd vidtagits och riskbedömning efter åtgärd.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Risk** | | **Initial riskbedömning** | | | **Åtgärd genomförd?** | **Riskbedömning efter åtgärd** | | |
| **Risk-id** | **Beskrivning** | **Allvarlighetsgrad** | **Sannolikhet** | **Riskpoäng** |  | **Allvarlighetsgrad** | **Sannolikhet** | **Riskpoäng** |
|  | ***Projektrisker*** |  |  |  |  |  |  |  |
| RP1 | Kravbilden är otydlig | 4 | 3 | 12 | JA | 4 | 2 | 8 |
| RP2 | Otillräcklig nytta för användare | 5 | 1 | 5 | NEJ | 5 | 1 | 5 |
| RP3 | Kan ej få fram önskad funktionalitet inom avdelad budget. | 3 | 3 | 9 | JA | 3 | 2 | 6 |
| RP4 | Brist på engagemang för projektet från användarna | 4 | 2 | 8 | NEJ | 4 | 2 | 8 |
| RP5 | Kraven missuppfattas av utvecklingsgruppen | 4 | 3 | 12 | JA | 4 | 1 | 4 |
| RP6 | Användning av ny/oprövad teknik | 3 | 2 | 6 | NEJ | 3 | 2 | 6 |
| RP7 | Brist på rätt kompetens hos utvecklingsgruppen | 5 | 1 | 5 | NEJ | 5 | 1 | 5 |
|  | ***Kvalitetsrisker*** |  |  |  |  |  |  |  |
| RK1 | Dålig stabilitet/upptid | 4 | 3 | 12 | JA | 4 | 1 | 4 |
| RK2 | Stor mängd buggar | 3 | 3 | 9 | JA | 3 | 2 | 6 |
| RK3 | Otillräcklig prestanda – långa svarstider | 3 | 2 | 6 | NEJ | 3 | 2 | 6 |
| RK4 | Felaktigheter i data som hanteras | 5 | 2 | 10 | JA | 5 | 1 | 5 |
| RK5 | Data blir korrupt eller förstörs | 5 | 2 | 10 | JA | 5 | 1 | 5 |
|  | ***Säkerhetsrisker*** |  |  |  |  |  |  |  |
| RS1 | Ej behörig användare kan logga in i systemet | 5 | 3 | 15 | JA | 5 | 1 | 5 |
| RS2 | Otillåten åtkomst av data | 5 | 3 | 15 | JA | 5 | 1 | 5 |