Sikkerhets- og risikostyringsportal – Risikovurderingsrapport

Sikkerhetsanalytiker Echomedic prosjektteam

LEDEROPPSUMMERING

1.1. Oversikt over vurderingen

Dette dokumentet presenterer en grundig risikovurdering av informasjonssikkerhet for Echomedics foreslåtte portal for sikkerhets- og risikostyring. Vurderingen er gjennomført i samsvar med GDPR (General Data Protection Regulation), Normen (regelverk for informasjonssikkerhet i den norske helse- og omsorgssektoren) og risikostyringstilnærmingen i ISO/IEC 27005:2022.

Risikovurderingen dekker alle aspekter av den foreslåtte portalen, inkludert:

- Nettbasert brukergrensesnitt (Angular/React-frontend)
- Mekanismer for brukerautorisering og autentisering
- Risikoregistermodulen som brukes til å registrere og overvåke sikkerhetstrusler
- Et bibliotek med sikkerhetspolicyer og -prosesser
- Backend REST API (Express/Node.js)
- PostgreSQL-databaseinfrastruktur
- Funksjonalitet for logging og overvåking
-

1.2 Hovedfunn

Totalt antall identifiserte risikoer: 15

Fordeling av risikonivåer:

CRITICAL (RED)	4	27%

HIGH (YELLOW)	10	67%
LOW (GREEN)	1	6%

Fordeling etter risikokategori:

- Tekniske risikoer: Ni (60 %)
- Organisatoriske risikoer: Fire (27 %)
- Prosessrisikoer: To (13 %)
- Juridiske og personvernrelaterte risikoer: Én (inkludert i organisatoriske risikoer)

Nåværende sikkerhetsnivå:

- Etterlevelse av ISO 27001: Omtrent 35 % (betydelige mangler identifisert)
- Etterlevelse av Normen: Rundt 40 % (kritiske kontroller mangler)
- Etterlevelse av GDPR: Omtrent 45 % (utilstrekkelige personverntiltak)

1.3. Sammendrag av kritiske risikoer

Før systemet tas i bruk må følgende fire KRITISKE risikoer håndteres:

RISIKO R001: Svak passordsikkerhet (Score: 9/9)

Problem:

Brukere kan opprette svake passord, som for eksempel «123456», noe som gjør kontoer sårbare for brute force-angrep.

Konsekvenser:

- Uautorisert tilgang til pasientdata
- Brudd på GDPR artikkel 32, som kan medføre bøter på opptil 20 millioner euro
- Tap av pasienttillit og betydelig omdømmeskade

Tiltak / løsning:

- Pålegge passord med minimum 12 tegn og krav til kompleksitet
- Konto låses etter fem mislykkede innloggingsforsøk
- Innføre passordutløpspolicy og passordstyrkemåler

Estimert implementeringstid: 16 timer

RISIKO R003: Ukryptert datalagring (Score: 9/9)

Problem:

Sensitiv pasientinformasjon lagres i databasen i klartekst uten kryptering.

Konsekvenser:

- Direkte brudd på GDPR artikkel 32
- Ved et datainnbrudd må hendelsen rapporteres innen 72 timer
- Potensielle bøter på opptil 20 millioner euro eller 4 % av global omsetning
- Alvorlig omdømmeskade

Tiltak / løsning:

- TLS 1.3 for data under overføring
- AES-256-kryptering av alle sensitive data lagret i databasen
- Sikker nøkkelhåndtering (for eksempel AWS KMS eller Azure Key Vault)

Estimert implementeringstid: 32 timer

RISIKO R004: Manglende tofaktorautentisering (Score: 9/9)

Problem:

Administrator-kontoer er kun beskyttet med passord og mangler en ekstra autentiseringsfaktor.

Konsekvenser:

- Dersom administratorpassord kompromitteres, kan hele systemet overtas
- Angripere kan endre risikovurderinger, slette logger og få tilgang til alle data
- Manglende beskyttelse mot phishing-angrep

Tiltak / løsning:

- Gjøre tofaktorautentisering (2FA) obligatorisk for alle administratorkontoer
- Implementere TOTP-løsninger (Google Authenticator, Authy)
- Bruke gjenopprettingskoder for kontogjenoppretting

Estimert implementeringstid: 20 timer

RISIKO R009: Usikre API-endepunkter (Score: 9/9)

Problem:

REST API-endepunkter er tilgjengelige uten autentisering, noe som muliggjør direkte manipulering av data.

Konsekvenser:

- Alle sikkerhetsbegrensninger i frontend kan omgås
- Alle som kjenner til URL-er kan lese eller endre data
- Manglende sporbarhet og revisjonslogg for datatilgang

Tiltak / løsning:

- Innføre JWT-tokenbasert autentisering på alle API-endepunkter

- Begrense trafikk til maks 100 forespørsler per minutt (rate limiting)
- Tvinge bruk av HTTPS på alle forbindelser

Estimert implementeringstid: 24 timer

1.4. Strategi for risikoreduksjon

Etter implementering av alle foreslåtte risikoreduserende tiltak:

	Before	After
CRITICAL Risks (RED)	4	0
HIGH Risks (YELLOW)	10	3
LOW Risks (GREEN)	1	12
Total Risk Score	96	38
Risk Reduction	-	60%
ISO 27001 Compliance	35%	85%
Normen Compliance	35%	90%
GDPR Compliance	45%	95%

2. INNLEDNING

2.1 Formål

Formålet med denne risikovurderingen er å:

1. Identifisere informasjonssikkerhetsrisikoene som Echomedics portal for sikkerhets- og risikostyring står overfor, inkludert risikoer knyttet til konfidensialitet av pasientdata, systemtilgjengelighet, regulatorisk etterlevelse og organisasjonens omdømme.
2. Analysere sannsynlighet og mulig konsekvens for hver identifiserte risiko gjennom en systematisk vurdering av trusselkilder, sårbarheter og angrepsscenarioer.
3. Fastsette behandlingsprioriteter basert på alvorlighetsgrad, etterlevelseskrav og forretningsmessig påvirkning ved å evaluere risikoene opp mot forhåndsdefinerte kriterier.
4. Foreslå hensiktsmessige og kostnadseffektive risikoreduserende tiltak i tråd med bransjens beste praksis, GDPRs prinsipper for personvern, Normen for helsesektoren og sikkerhetskontroller i ISO/IEC 27001:2022.
5. Gi et grunnlag for velinformerte beslutninger knyttet til sikkerhet og ressursallokering, slik at Echomedic kan nå sitt mål om å etablere et modent og strukturert styringssystem for informasjonssikkerhet.

Denne vurderingen støtter Echomedics strategiske mål om å etablere et systematisk rammeverk for kontinuerlig risikostyring og demonstrere modenhet innen informasjonssikkerhetsstyring. Dette bidrar til å bygge tillit hos pasienter, samarbeidspartnere og interessenter, sikre etterlevelse av GDPR ved behandling av pasientdata og legge grunnlaget for fremtidig ISO 27001-sertifisering.

2.2 Omfang

Innenfor omfanget (IN SCOPE):

Denne risikovurderingen omfatter følgende elementer av Echomedics sikkerhetsportal:

Applikasjonslag:

- Frontend webapplikasjon basert på Angular- eller React-rammeverket
- Backend REST API (Express-rammeverk med Node.js)
- Funksjonalitet for risikoregister (opprette, lese, oppdatere og slette)
- Dokumenthåndteringssystem og policybibliotek
- Grensesnitt for brukeradministrasjon
- Dashbord- og rapporteringsfunksjoner

Infrastrukturlag:

- Datalagring og PostgreSQL-databaseserver

- Nettverksarkitektur og tilkobling
- Webserver og applikasjonsdriftsmiljø
- Skyinfrastruktur (on-premises, AWS eller Azure)

Sikkerhetsdomener:

- Autentiseringsmekanismer (passordhåndtering, sesjonshåndtering, innlogging)
- Tilgangskontroll og autorisasjon (rollebaserte rettigheter)
- Databeskyttelse (sikker lagring, kryptering i transport og i hvile)
- Applikasjonssikkerhet (sikker kode, input-validering)
- API-sikkerhet (HTTPS, rate limiting og autentisering)
- Overvåking og logging (sikkerhetshendelser, revisjonsspor)
- Backup og katastrofegjenoppretting
- Hendelseshåndtering og kontinuitetsplanlegging

Dataressurser:

- Helseopplysninger og pasient-ID-er (dersom systemet behandler dette)
- Personopplysninger (e-post, navn, roller) og brukerlegitimasjon
- Data fra risikovurderinger og sikkerhetsregistre
- Sikkerhetspolicyer og prosedyrer
- Revisjonslogger og systemlogger
- Kildekode og konfigurasjonsfiler
- Kryptografiske sertifikater og nøkler

Etterlevelseskrav:

- ISO/IEC 27001:2022 – Ledelsessystem for informasjonssikkerhet
- Normen – Informasjonssikkerhet i den norske helsesektoren
- GDPR – Personvernforordningen (EU) 2016/679
- Personopplysningsloven og helsespesifikke forskrifter

Utenfor omfanget (OUT OF SCOPE):

Denne vurderingen inkluderer ikke:

- Eksisterende eldre systemer og applikasjoner hos Echomedic
- Interne prosesser hos tredjepartsleverandører (kun grensesnitt vurderes)
- Fysisk adgangskontroll og kontorsikkerhet
- HR-prosesser (ansettelseskontrakter, bakgrunnssjekker)
- Juridiske og kontraktsmessige forhold utover tekniske sikkerhetstiltak
- Finansielle og forretningsmessige risikoer som ikke er direkte knyttet til informasjonssikkerhet

- Markedsføring og forretningsutviklingsaktiviteter

2.3 Regulatorisk kontekst

Echomedic opererer i et strengt regulert miljø, noe som stiller høye krav til informasjonssikkerhet.

ISO/IEC 27001:2022 – Informasjonssikkerhetsstyring

ISO 27001 er den internasjonale standarden for ledelsessystemer for informasjonssikkerhet (ISMS).

Viktige krav inkluderer:

- En systematisk tilnærming til håndtering av sensitiv informasjon
- Risikobasert identifisering og håndtering av sikkerhetstrusler
- 93 sikkerhetskontroller fordelt på 14 domener (Vedlegg A)
- Kontinuerlig overvåking, evaluering og forbedring
- Omfattende dokumentasjon av policyer og prosedyrer
- Ledelsesforankring og tilstrekkelig ressursallokering

Relevante kontrollkategorier i Vedlegg A:

- A.5 Organisatoriske kontroller (37 kontroller)
- A.6 Menneskelige kontroller (8 kontroller)
- A.7 Fysiske kontroller (14 kontroller)
- A.8 Tekniske kontroller (34 kontroller)

Fordeler for Echomedic:

- Internasjonal anerkjennelse i helsesektoren
- Konkurransefortrinn i anbudsprosesser
- Strukturert rammeverk for sikkerhetsstyring
- Økt tillit hos partnere og kunder
- Dokumentert aktsomhet overfor regulatorer og revisorer

Normen – Informasjonssikkerhet i helsesektoren

Normen fastsetter spesifikke sikkerhetskrav for norske helseorganisasjoner.

Relevante områder:

4.1 Sikkerhetsbevissthet og opplæring

- Årlig obligatorisk opplæring for alle ansatte
- Spesialisert opplæring for håndtering av helseopplysninger
- Bevissthet rundt phishing, sosial manipulering og interne trusler

4.2 Autentisering og tilgangskontroll

- Sterk autentisering for alle brukere
- Obligatorisk multifaktorautentisering for privilegerte kontoer
- Rollebasert tilgangskontroll (RBAC) og kvartalsvise tilgangsrevisjoner
- Prinsippet om minste privilegium
- Umiddelbar fjerning av tilganger ved avsluttet arbeidsforhold

4.3 Konfidensialitet og kryptering

- Kryptering av pasientdata i hvile med sterke algoritmer (AES-256)
- Kryptering av data i transitt (minimum TLS 1.2)
- Sikker nøkkelhåndtering
- Forebygging av uautorisert deling av helseopplysninger

4.4 Tilgjengelighet og kontinuitet

- Regelmessig testing av backup og gjenoppretting
- Katastrofeberedskapsplaner
- Definerte RTO-krav for kritiske systemer
- Beskyttelse mot DDoS-angrep

4.5 Sikker utviklingslivssyklus

- OWASP-baserte prinsipper for sikker koding
- Integrering av sikkerhet i designfasen
- Sårbarhetshåndtering og rask patching
- Kodegjennomgang og sikkerhetstesting før produksjonssetting
- Endringshåndtering med sikkerhetsvurdering

4.6 Overvåking og logging

- Fullstendig logging av all tilgang til pasientdata
- Overvåking og varsling av sikkerhetshendelser
- Minimum 12 måneders logglagring
- Beskyttelse av loggintegritet
- Regelmessig gjennomgang av logger

4.7 Leverandør- og tredjepartsstyring

- Sikkerhetsvurdering av leverandører før avtaleinngåelse
- Databehandleravtaler med sikkerhetskrav
- Regelmessige revisjoner
- Rett til revisjon og hendelsesrapportering

GDPR – Personvernforordningen

GDPR stiller strenge krav til behandling av personopplysninger.

Viktige artikler:

Artikkel 5 – Behandlingsprinsipper

Lovlighet, rettferdighet og åpenhet; formålsbegrensning; dataminimering; riktighet; lagringsbegrensning; integritet og konfidensialitet; ansvarlighet.

Artikkel 25 – Innebygd personvern og personvern som standard

Tekniske og organisatoriske tiltak fra designfasen; personvern som standardinnstilling, pseudonymisering og minimering.

Artikkel 32 – Sikkerhet ved behandlingen

Kryptering og pseudonymisering; sikring av konfidensialitet, integritet og tilgjengelighet; regelmessig testing og evaluering.

Artikkel 33–34 – Varsling av brudd

Varsling til tilsynsmyndighet innen 72 timer; varsling av berørte registrerte ved høy risiko.

Artikkel 35 – DPIA

Påkrevd ved høy risiko; vurdering av nødvendighet, forholdsmessighet og risikoreduserende tiltak.

Artikkel 37 – Personvernombud (DPO)

Obligatorisk ved behandling av helseopplysninger; uavhengig rolle med direkte rapportering til ledelsen.

Sanksjoner ved manglende etterlevelse:

- Opptil 20 millioner euro eller 4 % av global omsetning
- Omdømmeskade og tap av tillit
- Tilsyn og mulige erstatningskrav

Krav Echomedic må oppfylle:

- Samtykkebasert databehandling
- Lovlig behandlingsgrunnlag
- Rett til innsyn, sletting og dataportabilitet
- Tydelige personvernerklæringer
- Utnevnelse av DPO
- Behandlingsprotokoller (artikkel 30)
- Databehandleravtaler
- Beskyttelse ved internasjonale dataoverføringer

---

3. RISIKOVURDERINGSMETODIKK

3.1 Rammeverk og standarder

Denne risikovurderingen er basert på anerkjente internasjonale standarder.

Primært rammeverk:

- ISO/IEC 27005:2022 – Risikostyring for informasjonssikkerhet
    - Støtter ISO 27001
    - Fremmer en risikobasert tilnærming

Støttestandarder:

- ISO/IEC 27001:2022 og ISO/IEC 27002:2022
- NIST SP 800-30 Rev. 1
- NIST Cybersecurity Framework (CSF)

Bransjens beste praksis:

- OWASP Top 10 Web Application Security Risks (2021)
- OWASP Application Security Verification Standard (ASVS)
- CIS Controls v8
- SANS Top 25 mest kritiske programvarefeil

3.2 Risikovurderingsprosess

Risikoevalueringen følger en strukturert firefaset prosess i henhold til ISO 27005.

Fase 1: Etablering av kontekst

Aktiviteter:

- Definere mål og omfang
- Identifisere interessenter
- Fastsette vurderingskriterier
- Definere akseptabel risiko

Metoder:

- Gjennomgang av tilsvarende helserelaterte risikovurderinger
- Intervjuer med prosjektmedlemmer
- Dokumentanalyse
- Analyse av regulatoriske krav

Resultater:

- Definert omfang
- Risikokriteriematrise
- Interessentoversikt

Fase 2: Risikoidentifisering

Aktiviteter:

- Kartlegging av informasjonsverdier
- Identifisering av trusler og sårbarheter
- Evaluering av eksisterende kontroller
- Dokumentasjon av angrepsscenarioer

Metoder:

- Tverrfaglig workshop med åtte deltakere (desember 2024)
- STRIDE-trusselmodellering
- Angrepstreanalyse
- Kodegjennomgang
- OWASP Top 10-sjekkliste
- Bransjerapporter

Resultater:

- Klassifisert aktivainventar
- Trussel- og sårbarhetskatalog
- 15 identifiserte risikoer

Fase 3: Risikoanalyse

Aktiviteter:

- Vurdere sannsynlighet og konsekvens
- Beregne risikonivå
- Evaluere kontrollers effektivitet

Metoder:

- Kvalitativ analyse (1–3-skala)
- Ekspertvurderinger
- Bransjedata (Verizon DBIR, IBM)
- ISO 27001-gap-analyse

Resultater:

- Begrunnede sannsynlighetsscorer
- Konsekvensanalyse
- Risikonivå (1–9)
- Risikoklassifisering (RØD, GUL, GRØNN)

Fase 4: Risikovurdering og behandling

Aktiviteter:

- Sammenligne risiko med akseptkriterier
- Prioritere tiltak
- Velge behandlingsstrategi
- Utarbeide tiltak og estimere rest-risiko

Metoder:

- Risikomatriser
- Kost–nytte-analyse
- Kontrollutvalg basert på ISO 27001 Vedlegg A
- Rest-risikoberegning

Resultater:

- Prioritert risikoregister
- Tiltaksplan med tidslinje
- Kostnads- og ressursestimater
- Dokumentert reduksjon i risiko

3.3 Kriterier for risikovurdering

VURDERING AV SANNSYNLIGHET (SKALA 1–3)

Score	Level	Description

1	Unlikely	Hendelsen er lite sannsynlig å inntreffe i nær fremtid. Årlig sannsynlighet er mindre enn 10 %. Forventet frekvens: Hvert tiende år eller sjeldnere Eksempler inkluderer innsidersabotasje (med tilstrekkelige kontroller på plass), målrettede angrep fra nasjonalstater mot små organisasjoner og naturkatastrofer som rammer datasentre.
2	Possible	En hendelse kan inntreffe under bestemte omstendigheter. Årlig sannsynlighet: 10–50 % Forventet frekvens: Hvert annet til tiende år Eksempler SQL-injeksjon dersom kode ikke er korrekt validert; maskinvarefeil uten redundans; og målrettede phishing-kampanjer.
3	Likely	Hendelsen forventes å inntreffe hyppig. Årlig sannsynlighet: Over 50 % Forventet frekvens: Flere ganger årlig

		Eksempler: Automatiserte sårbarhetsskanninger; phishing-e-poster rettet mot ansatte; og brute force-forsøk mot svake passord.

Følgende faktorer tas i betraktning ved vurdering av sannsynligheten for at en hendelse inntreffer:

- Historiske hendelsesdata (interne sikkerhetsbrudd og bransjetrender)
- Kjente sårbarheter og eksponeringsnivå
- Trusselaktørers kapasitet, ressurser og motivasjon
- Størrelsen på angrepsflaten og hvor lett den er å utnytte
- Effektiviteten av eksisterende forebyggende kontroller
- Miljøfaktorer (internett-eksponerte systemer versus interne systemer)
- Bransjespesifikk målretting (helsetjenester er et høyverdimål)

KONSEKVENSVURDERING (SKALA 1–3)

Score	Level	Consequences
1	Low	Operasjonell: Mindre enn 10 brukere ble berørt. Tjenesteavbruddet varte i mindre enn 4 timer. Det finnes tilgjengelige midlertidige løsninger; det er kun mindre ulemper og ingen permanent datatap. Økonomisk: Ingen vesentlig økonomisk påvirkning på virksomheten.

		Ingen behov for å melde forsikringskrav. OMDØMME: Hendelsen er liten og avgrenset. Kun lokal eller intern påvirkning. Ingen medieomtale. Minimal påvirkning på tillit. ETTERLEVELSE: Ingen krav om rapportering til tilsynsmyndigheter. Mindre brudd på interne retningslinjer.
2	Low	ETTERLEVELSE: Krav om rapportering til tilsynsmyndigheter. Mulige advarsler eller mindre sanksjoner. Avvik i ISO 27001-revisjon (kan korrigeres). Behov for økt oppfølging og tilsyn.
3	High	OPERASJONELL: Mer enn 100 brukere ble berørt. Tjenesteavbrudd som varer lenger enn 24 timer.

		Alvorlig datatap eller datakorrupsjon. Et betydelig databrudd som involverer mer enn 100 poster. En trussel mot virksomhetens kontinuitet. OMDØMME: Alvorlig skade på selskapets omdømme. Oppmerksomhet fra nasjonale og internasjonale medier. Tap av pasient- og kundetillit, som er vanskelig å gjenopprette. Konkurranseulempe. Tap av forretningsmuligheter. ETTERLEVELSE: Varsling av GDPR-brudd må gis innen 72 timer. Mulig suspensjon av lisenser eller regulatoriske sanksjoner. Rettlige skritt fra berørte parter; risiko for at ISO 27001-sertifisering trekkes tilbake eller settes i fare; samt flere regulatoriske konsekvenser. investigations. PASIENSIKKERHET: Mulige konsekvenser for pasientbehandling eller pasientsikkerhet. Kompromittert konfidensialitet for helseopplysninger.

		Brudd på taushetsplikten mellom lege og pasient.

RISK SCORING MATRIX

Risk Score = Likelihood × Impact

IMPACT →

3 🟢	6 🟡	9 🔴
2 🟢	4 🟡	6 🟡
1 🟢	2 🟢	3 🟡

3.4 Tilnærming til risikobehandling

Basert på organisasjonens risikoappetitt og kost–nytte-analyse velges én av fire behandlingsstrategier for hver identifiserte risiko:

Behandlingsalternativ 1: UNNGÅ (AVOID)

Forklaring:

- Eliminere risikokilden fullstendig
- Endre systemarkitekturen for å fjerne sårbarheten
- Avslutte risikofylt atferd
- Velge en alternativ løsning med lavere risiko

Når brukes dette:

- Risikoen kan ikke reduseres tilstrekkelig og er uakseptabel
- Kostnaden ved risikoreduserende tiltak overstiger nytten av aktiviteten
- Det finnes alternative metoder med lavere risikoprofil
- Aktiviteten er ikke nødvendig for kjernevirksomheten

Eksempler:

- Ikke implementere en risikofylt funksjon som ikke er nødvendig
- Beslutte å ikke lagre bestemte typer sensitiv informasjon
- Erstatte egenutviklede løsninger med velprøvde tredjepartsløsninger

---

Behandlingsalternativ 2: REDUSERE (MITIGATE)

Forklaring:

- Implementere sikkerhetstiltak for å redusere sannsynlighet eller konsekvens
- Den mest brukte tilnærmingen for håndtering av tekniske risikoer
- Benytte sikkerhetskontroller fra ISO 27001 Vedlegg A
- Bruke flere lag med beskyttelse (defense in depth)

Når brukes dette:

- Risikoen er høyere enn akseptabel, men tiltak er mulig
- Det finnes kostnadseffektive kontroller
- Gjenværende risiko vil være akseptabel etter tiltak
- Aktiviteten er nødvendig for sentrale forretningsprosesser

Eksempler:

- Implementere input-validering for å redusere risiko for SQL-injeksjon
- Innføre kryptering for å redusere konsekvensen av databrudd
- Implementere multifaktorautentisering for å redusere kontokompromittering

Typer kontroller:

- FOREBYGGENDE: Hindrer hendelser før de oppstår (brannmurer, tilgangskontroll)
- DETEKTIVE: Oppdager hendelser når de inntreffer (logging, overvåking, IDS)
- KORRIGERENDE: Reduserer konsekvens etter hendelser (backup, hendelseshåndtering)

Behandlingsalternativ 3: OVERFØRE (TRANSFER / SHARE)

Forklaring:

- Overføre deler av risikoen til en tredjepart
- Bruk av kontrakter, forsikring og outsourcing
- Finansiell og operasjonell belastning deles, men risikoen fjernes ikke helt

- Ansvar kan overføres til forsikringsselskap eller leverandør

Når brukes dette:

- Organisasjonen mangler nødvendig spesialkompetanse
- Egen håndtering er for kostbar
- Finansiell risiko må fordeles eller sikres
- Tjenestenivåavtaler (SLA) gir tilstrekkelige garantier

Eksempler:

- Bruk av skyplattformer med SLA (AWS, Azure)
- Cyberforsikring for økonomisk beskyttelse ved databrudd
- Engasjere MSSP (Managed Security Service Provider) for sikkerhetsdrift
- Ansvarsbestemmelser i leverandørkontrakter

Begrensninger:

- Omdømmerisiko kan ikke fullt ut overføres
- GDPR pålegger fortsatt organisasjonen det overordnede ansvaret
- Krever kontinuerlig oppfølging og kontroll av leverandører

Behandlingsalternativ 4: AKSEPTERE (ACCEPT)

Forklaring:

- Risikoen anerkjennes og det iverksettes ingen umiddelbare tiltak
- Risikoen ligger innenfor akseptable rammer
- Må dokumenteres og godkjennes av ledelsen
- Krever løpende overvåking

Når brukes dette:

- Risikonivået er lavt (GRØNN) og innenfor risikoappetitten
- Potensiell skade overstiger kostnaden ved tiltak
- Det finnes ingen gjennomførbare eller kostnadseffektive kontroller
- Risikoen er eksplisitt akseptert av toppledelsen

Eksempler:

- Akseptere lav sannsynlighet for leverandørbrudd hos pålitelig leverandør
- Akseptere lav risiko knyttet til historiske funksjoner som er avviklet
- Akseptere rest-risiko etter at alle rimelige tiltak er implementert

Forutsetninger:

- Formell godkjenning av risikoaksept på riktig ledelsesnivå
- Dokumentert begrunnelse for aksept

- Regelmessig revurdering (minst én gang årlig)
- Overvåking av endringer i trusselbildet

---

4. IDENTIFISERING AV EIENDELER

Basert på deres betydning for Echomedics virksomhet og konsekvensene ved kompromittering, er kritiske eiendeler identifisert og kategorisert som følger:

4.1 Inventar over informasjonsverdier

A-01	Patient Data	Identifiers, medical data, treatment histories, diagnoses, and personal health information	CONFIDENTIAL (Highest)	Data Controller
A-02	User Credentials	2FA secrets, session data, authentication tokens, hashes of passwords, and usernames	CONFIDENTIAL	Security Team
A-03		determined security threats, evaluations,	INTERNAL	Security Manager

	Risk Register Data	vulnerability information, and mitigation strategies		
A-04	Security Policies	SOPs, security standards, incident response protocols, and access control rules	INTERNAL	Security Manager
A-05	System Logs	Application logs, audit trails, security events, and access logs	INTERNAL	IT Ops
A-06	Application Code	Source code, configuration files, deployment scripts, and API documentation	INTERNAL	Dev Team
A-07	Cryptographic Keys	Secrets, signing keys, SSL/TLS certificates, encryption keys, and API keys	RESTRICTED (Absolute Highest)	Security Team

4.2 System Assets

ID	Asset Name	Description	Criticalitycd
S-02	Web Application (Frontend)	Reports, dashboards, forms, and user-facing interfaces (Angular and React)	HIGH
S-03	API Server (Backend)	Data processing, integrations, core business logic, and REST API (Node.js/Express)	CRITICAL
S-04	Database Server	PostgreSQL database, single source of truth, and permanent data storage	CRITICAL
S-05	Authentication Service	Password verification, token creation, sessions, login, and 2FA	CRITICAL
S-06	Logging Infrastructure	Audit trails, security logs, and SIEM integration (planned)	HIGH

S-07	Backup System	Disaster recovery, offsite storage, automated backups, and restoration capabilities	HIGH

Definisjoner av eiendelsklassifisering:

KONFIDENSIELL (Høyeste beskyttelsesnivå):

- Kryptering er påkrevd både i transitt og ved lagring
- Tilgang er begrenset til autorisert personell med tjenstlig behov
- Grundig revisjonslogging av all tilgang
- Kan ikke distribueres eksternt uten tillatelse
- Data Loss Prevention (DLP)-tiltak er implementert
- Eksempel: Brukerlegitimasjon og pasientdata

Intern (Middels beskyttelsesnivå):

- Tilgjengelig for ansatte med forretningsmessig behov
- Ekstern deling kun med godkjenning
- Tilgang bør loggføres
- Standard rutiner for backup og gjenoppretting
- Eksempler: Sikkerhetsregler og risikoregistre

Begrenset (Absolutt høyeste beskyttelsesnivå):

- Svært begrenset tilgang (vanligvis 1–2 personer)
- Anbefalt bruk av maskinvarebaserte sikkerhetsmoduler (HSM)
- To-personers kontroll og delt kunnskap der det er mulig
- All elektronisk kommunikasjon skal alltid være kryptert
- Fysiske sikkerhetstiltak er påkrevd
- Eksempel: Rotsertifikater og hovedkrypteringsnøkler