

Access Control Policy

Formålet med dette er å sikre at kun autoriserte personer har tilgang til systemer og informasjon i Echomedic, og at all tilgang er basert på kun de som faktisk trenger og i minste privilegium.

Referanser:

- ISO/IEC 27001:2022 Annex A – Controls A.5 OG A.9 (Access Control)
- GDPR Art. 32 – Sikring av personopplysninger
- Normen: Kap. 2. Normens krav til tilgangsstyring

Omfang: Policyen gjelder for alle ansatte, innleide konsulenter og leverandører som i sitt arbeid får tilgang til Echomedic sine systemer og data.

Roller:

Rolle	Beskrivelse	Tilgang
Klinisk Personell	Leger, sykepleiere, terapeuter	Pasientdata, Journalsystem, medisinske rapporter
Administrasjon	Ledelse, HR, Økonomi	Personaldata, økonomi, kontrakter
Systemadministrator	IT-personell med drift- og vedlikeholdsansvar	Uttalt systemtilgang, loggtilgang og sikkerhetsverktøy
Leverandører	Eksterne drifts- eller supportpartnere	Begrenset og midlertidig tilgang via autentiserte sesjoner

Tilgangsnivåer

1. Individuelle (ingen delte kontoer)
2. Begrunnede (De som har behov)
3. Godkjent av ansvarlig leder
4. Dokumentert i Tilgangsregister

Tilgang til pasientdata skal følge helsepersonelloven og Normen.

Passordpolicy

- Skal være minimum 12 tegn
- Skal inneholde tall, symboler og store/små bokstaver
- Rotasjon hver 160. dag
- Tidligere 5 passord skal ikke gjenbrukes
- Multifaktor skal benyttes på eksterne innlogginger og cloud-systemer
- Passord skal aldri lagres i klartekst
- Passordadministrator som «Bitwarden» anbefales sterkt

2FA

Echomedic krever 2FA ved:

- Innlogging til journalsystem
- Tilgang til pasientdata via fjernkobling
- Cloud-baserte systemer som Azure eller AWS

Periodisk tilgangsrevisjon

Utføres minimum hver 6. måned og disse punktene her skal kontrolleres:

- Feilaktige og ubrukte brukerkontoer
- Tilgangsnivå i forhold til rolle
- Leverandør og testtilganger

Resultatet skal deretter dokumenteres og lagres i 2 år ifølge Normen Krav. Samt at tilganger fjernes umiddelbart ved fratredelse av stilling.

Logging & Monitoring Policy

Formål: Sikre sporbarhet, oppdage misbruk og kunne dokumentere avvik.

Omfang: Gjelder alle systemer som håndterer pasientdata, personaldata og sensitiv virksomhetsinformasjon.

Hva som skal logges:

- Innloggingsforsøk Riktig/Feil
- Tilgang til pasientjournaler og sensitive mapper
- Endringer i brukerrettigheter
- Installering av applikasjoner og oppdateringer
- Sikkerhetshendelser (Virus, malware, IPS, brannmutriggers)
- API Kall mot eksterne API er med sensitive funksjoner

Loggene skal være :

- Manipulasjonssikret
- Tidsstemplet
- Kryptert i hvile og transitt

Hvem har tilgang til loggene:

- CTO/Sikkerhetsleder
- Godkjent driftsleverandør med signert databehandleravtale
- Tilgangen skal være sporbar og begrunnet
- Ingen kliniske brukere eller saksbehandlere skal ha tilgang.

Lagringstid for Logger:

- Standard lagringstid er 12 måneder
- Ved hendelser er det minimum 5 år
- GDPR: Kun lagring av loggdata nødvendig for sikkerhet og revisjon

Overvåking av logger

Daglig automatisk monitorering

Månedsrappport med statistikk (forsøk på uautorisert tilgang, misbruk)

Skal varsles ved:

- Mistenkelig trafikk
- Gjentatte mislykkede innlogginger
- Tilgang til journaler uten klar behandlingsrelasjon ifølge Normen Krav.

Alle alarmsignaler skal utredes innen 24 timer.

Incident Management Policy

Formål: Er å sikre rask håndtering av sikkerhetshendelser som kan påvirke pasientdata, drift eller kvalitet.

Hvordan oppdage hendelser:

- Varslinger fra verktøy som IDS/IPS og logganaylse.
- Avviksmeldinger fra ansatte
- Manuelle revisjoner
- Varsling fra leverandører
- Pasienthenvendelser med mulige feil i journal.

Hvordan hendelser skal rapporteres:

Alle ansatte er pliktige til å rapportere sikkerhetsavvik til sikkerhetsansvarlige, Drift og ledelsen.

Rapporten skal bestå av 4 punkter:

1. Tidspunkt
2. Hva som ble oppdaget
3. Berørte personopplysninger
4. Risiko for pasientdata

Hvem som håndterer hendelser:

1. Sikkerhetsleder som har overordnet ansvar
2. IT-Driftspartner/Leverandør som har ansvar for teknisk analyse
3. Databehandleransvarlig må gå gjennom GDPR og gjøre vurderinger
4. Ledelsen må ta en beslutning på hvilke tiltak som bør etableres

Disse sikkerhetspolicyene gjelder for echomedic casen og skal derfor sikre at virksomheten behandler pasientdata og all annen viktig og sensitiv informasjon i samsvar med kravene i ISO/IEC 27001, Normen for informasjonssikkerhet i helse og omsorgssektoren og gjeldende lovverk som GDPR Art. 32 om sikkerhet ved behandling av personopplysninger. Policyen skal legge et grunnlag for forsvarlig tilgangsstyring, logging og overvåking, hendelseshåndtering, sikker lagring, sikker utvikling og bruk av IT utstyr. Dette gjelder for alle ansatte, innleide ressurspersoner og leverandører som arbeider med Echomedic typ systemer og opplysninger.

Referanser

- ISO/IEC 27001 Annex A.8: Logging og Monitoring
- GDPR Art. 32 (Sikkerhetstiltak)
- Normen Kap 5: Krav til sporbarhet og logging